DEPARTMENT OF THE AIR FORCE

AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GLM/LAL/98S-7

FEASIBILITY STUDY ON THE USE OF THE INTERNET FOR TRAFFIC OF UNCLASSIFIED DATA

THESIS

Alexandre L. Guerra
1st Lieutenant, Brazilian Air Force

Luiz Gustavo F. P. Silva
1st Lieutenant, Brazilian Air Force

AFIT/GLM/LAL/98S-7

AFIT/GLM/LAL/98S-7

FEASIBILITY STUDY ON THE USE OF THE INTERNET FOR TRAFFIC OF UNCLASSIFIED DATA

THESIS

Presented to the Faculty of the Graduate School of Logistics and Acquisition Management of the Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Logistics Management

Alexandre Lima Guerra, B.S.

1st Lieutenant, Brazilian Air Force

Luiz Gustavo F. P. Silva, B.S.

1st Lieutenant, Brazilian Air Force

September 1998

Preface

The basic motivation to start this research was the observation of the increasing use of Virtual Private Networking by the commercial sector to cut costs related to networking and improve integration along the supply-chain processes. The Brazilian Air Force, although responsible to cover the enormous area of the National territory, is not able to share resources and information across the units and depots of the Materiel Command. Perhaps, using this new technology to interconnect user units and depots, the Brazilian Air Force could be able to have a more tight control of aeronautical items and human resources involved in the process of maintenance and support of weapon systems.

Additionally, we felt that studying the aspects of networking security involved in the process of Information Warfare could contribute to the formation of a Brazilian Air Force nucleus responsible for emergency responses and for studying aspects of the modern Information Warfare arena. We expect that this research would help the Brazilian Air Force decision makers to understand that the use of the Internet to share resources can be beneficial in terms of cost, security, flexibility, and performance; and to call attention to the fact that a modern Air Force undoubtedly

needs to be prepared to the new challenges posed by Information Warfare.

This research is an extract of all the literature and researches we could gather in the period where we stayed in the Air Force Institute of Technology. We expected to perform some laboratory experiments in order to assess security and performance issues in controlled conditions. Unfortunately, due to the lack of time, those experiments could not be performed.

We would like to thank our thesis advisors, Major William L. Scott and Major Al Johnson, for the hours of advice and enlightening. We would like to thank the personnel of the DIRINFE and of the PAMASP for data provided to the thesis.

We also would like to express our gratitude to the friends of the International Military Student Office, Mrs. Annette Robb and Mrs. Lynn Curtis, for their constant support and fellowship.

Lt. Silva is very grateful beyond words to his family, his wife Leila and his daughter Alessandra, for the abdication of countless hours without husband and father, and for his friends for the support and contributions to this thesis.

Lt. Guerra would like to thank his parents, whose love and abnegation were the ultimate responsible for his coming to the Air Force Institute of Technology. He also would like to express a special gratitude to Gustavo, Leila, and Alessandra, whose friendship revealed to be his most valuable find of all he experienced in the United States.

Alexandre L. Guerra
Luiz Gustavo Figueiredo Pereira da Silva

(Page intentionally left in blank)

Table of Contents

Page

Page

(Page intentionally left in blank)

List of Figures

(Page intentionally left in blank)

List of Tables

Abstract

This research compares two possible networking methods for connecting all Brazilian Air Force Materiel Command units responsible for support and operation of Brazilian Air Force's weapons systems. The network includes the use of dedicated X.25 links, and the use of a Virtual Private Network using the Internet (TCP/IP) as the medium of transmission. The Brazilian Air Force Materiel Command, responsible to support operating units over a very large sparse territory, lacks an efficient media of computer communications, which makes it difficult to control the supply-chain channels of materiel present in each unit, depots, and warehouses. The network infrastructure necessary to solve this problem was studied, and two different scenarios were proposed. One uses the current level of technology based on dedicated X.25 environment, and the other uses the incipient Virtual Private Networking technology and the Internet as the communication medium. The results suggest that the Brazilian Air Force could be able to use the Internet and VPN technology in a moderated secure environment (C2 Level), and could save more than $

100,000 per month in comparison to the implementation of the same level of networking using the present X.25 model.

This study concludes that the BAF may benefit from the use of the VPN model in a secure and less costly environment, while maintaining the necessary flexibility and high performance to operate in the newly paradigm of distributed environments. Other implications for the Brazilian Air Force regarding Information Warfare issues and recommendations for further study are discussed.

FEASIBILITY STUDY ON THE USE OF THE INTERNET FOR TRAFFIC OF UNCLASSIFIED DATA

I. Introduction

Chapter Overview

The Brazilian Air Force's Computer Science and Statistics Directorate (DIRINFE) - which is responsible for setting the Brazilian Air Force's (BAF) computer policies - and the Air Traffic Directorate (DEPV) - which is responsible for operating BAF's computer networks - have recommended to all BAF units to avoid using the Internet as a primary medium of data communication. Instead, they have recommended the use of a leased data communications network based on the X.25 protocol.

This apparently was due to the perception of the Internet as an insecure and pervasive medium of data communications. Information Warfare issues, hacker attacks, and reliability concerns appear to be the major drivers for the policy of non-Internet networking on Defense-related organizations [1]. Major concerns relate to the theft of classified information, the disruption of C3 systems and weapon & platform control systems, and the disruption of logistics and other unclassified information systems [2].

Currently, the BAF employs six X.25 leased links of 9,600 bps each connecting hubs in São Paulo - SP, Brasília - DF, Recife - PE, Belém - PA, Manaus - AM, and Porto Alegre - RS to the concentrator in Rio de Janeiro (RJ) [3]. Additionally, satellite capability is available: eight channels of 64 KBPS; however, this capability is not yet being fully exploited. These links together represent the network connections between the major commands and principal depots of the Brazilian Air Force. Remote sites do not have direct access to these links, and they must rely on dial-up connections in order to be connected to any external network.

The Air Traffic Directorate has operated and maintained dedicated links (called BAF Wide Area Network - RCDMA) and satellite capabilities for the Materiel Command (DIRMA) networking requirements, but this network approach has not fully meet the increasing demand for traffic, speed, and reliability of data communications between the BAF units. It is proposed that by using the Internet for ordinary data communications - in conjunction with special software and hardware - the Brazilian Air Force Material Command could have a reliable, more flexible, less costly, and even more secure way to transmit and receive data between organizations.

Novell NetWare and Windows NT are the major servers' operating system used in BAF's local area networks (BAF-LAN), while mainframe computers operating MVS and Unix are used in some locations. Using the new developed Virtual Private Network (VPN) specifications, one should be able to leverage the Internet as a backbone for carrying IPX (Novell NetWare native network protocol), NetBEUI (Windows native network protocol), as well as TCP/IP (Transmission Control Protocol and Internet Protocol) remote access traffic. VPNs encrypt IP datagrams, use strong authentication and access control, and check data integrity to assure packets arrive at their destination unchanged. VPNs can reduce the costs of building and maintaining internal dial-up infrastructure or more expensive point-to-point Wide Area Network (WAN) links [4]. According to Hurwicz [5]:

> The Internet provides WAN communications more cheaply and more globally than a leased line, Frame Relay, or Asynchronous Transfer Mode (ATM) network. Unfortunately, it can't provide the security, bandwidth, or quality of service (QoS) guaranteed typically associated with private networks.

This study deals exactly with this point: the tradeoff between cost reduction and guaranteeing security and reliability of communications over the public network infrastructure through the use of virtual private networking.

In order to study the feasibility of using the Internet as a more cost-effective "corporate" backbone of data transmission by means of a virtual WAN, this research first addresses the current BAF's networking policy. Secondly, it describes the current state of the BAF Material Command information systems, networks, and links used to control aeronautical items. After that, the total cost of operation, including maintenance of the lines and equipment used by the Brazilian Air Force to all units of the Materiel Command is estimated. Security, performance, and reliability issues of the current model were also assessed in order to compare with potential alternative models of VPNs.

This chapter provides a background on networking and the BAF networking policy and describes the specific problem, research objectives, methodology, assumptions, scope and limitations, significance of research, and expected results.

Background

Computers have taken an increasing role in the way corporations and governments do business today. Information Systems have increased our capacity to do tasks better, in less time, and with greater accuracy. However, in order to integrate all information into one "information warehouse,"

one needs to connect information resources through computer networks.

There are several methods to make the connections between computers. In the past, the majority of the computer networks followed the specification of the X.25 model - heavily used by legacy systems. In this model, network connections were made through private lines - most of them dedicated lines - between servers and clients, or between local networks. One disadvantage of the X.25 approach is the considerable overhead that is justified only when there is a significant probability of error on any of the links in the network [6].

Another paradigm arose with the advent of the Transmission Control Protocol (TCP) and the Internet Protocol (IP) suite. This protocol suite grew out of defense research efforts (ARPANet) to design networks that were relatively bomb-proof [7, 8]. After being restricted to the research and academic community for more than 20 years, the Internet - the interconnection of computers all over the world using the TCP/IP protocols - has become the most widely used computer network in the world [9].

One characteristic of the Internet is scalability. Scalability can be defined as the capacity to support small, medium-sized, and large computer environments in the same

network. Therefore, organizations with massive computer resources (mainframes) or individuals with just a laptop computer are able to hook up to the Internet. The difference resides only in the way they are physically connected.

In general, large organizations are connected to the Internet backbone by high-performance links using fiber-optic cables. Individuals, small and mid-size organizations are generally connected to a third-party Internet Service Provider (ISP), who in turn is usually directly connected to the Internet backbone. Internet Service Providers charge users a fee for the network access. Depending on the desired traffic rate, the fee can be much lower than the fee applied to an exclusive link to the Internet.

One problem, however, of using the Internet to connect two computers is its - still desired - "open architecture." Perhaps one of the greatest benefits of the TCP/IP protocol is exactly its open architecture. However, without the proper security, the network becomes susceptible to hacker attacks, unwanted outside access, and denial of service attacks, which can compromise the network operability [10].

The Internet Engineering Task Force (IETF) has been working on a new TCP/IP specification, the so-called IPv6 or Secure IP (IPSEC). An immediate solution, however, is the

use of Virtual Private Networks (VPN) to create "extranets" over the Internet. This technique uses authentication and strong cryptography to create "arms" of networks throughout the Internet, and to put confidential data and mission-critical applications out of risk [11]. The United States Government has created an extranet prototype called the Extranet for Security Professionals (ESP), whose objective is given by the following citation:

> Provide the Nation better Security Service, Modernize the management of Security, Reduce the cost of doing business, Increase the Security Profession's credibility, and complain to the Smart Security PDD 29 (Presidential Decision Directive 29), while building the Security Infrastructure for the Next Millennium. [12]

This effort is sponsored by the US Department of the Air Force, NASA, and DARPA.

In the commercial sector, software and hardware vendors such as Microsoft, CentralPoint, Cisco, and IBM are working to deploy immediate VPN solutions. Microsoft recently released the Point-to-Point Tunneling Protocol (PPTP) for the Windows Operating System family. In addition, distributed computing using encrypted network layers (based on Sun's Java, Javabeans, CORBA or Microsoft's ActiveX, Active Server Pages, and DCOM) - an integral feature of extranets - has becoming more and more popular in application development.

In the United States, more and more carriers, such as MCI [13], AT&T, Sprint, GTE, UUNet, and CompuServe [14], are announcing Virtual Private Networking services as a commodity. Corporations such as MasterCard [15], the three big automotive companies (General Motors, Ford, and Chrysler) and small companies such as Mondavi [16, 17, 18, 19, 20] have implemented Internet-based solutions in order to cut transaction times and reduce the network cost of ownership and maintenance. In MasterCard's case, they actually upgraded their X.25 network to a virtual private network based on a mixed Internet Frame Relay technology. Tate [21] in her white paper "Internet Security: Can best practices overcome worst perils?" affirms that benefits in the use of extranets include:

> Reduction of operation and maintenance costs, improve in organization's efficiency of workflow applications, improved customer service, better data collection and distribution, faster and better decision-making, and lower costs for deploying client/server applications.

The Brazilian Air Force can probably achieve the same advantages in terms of cost and performance. This study not only deals with the implementation of a BAF's Virtual Private Network, but also with the feasibility of using the TCP/IP protocols in terms of cost, security and flexibility.

Research Objectives

The target audience of this research are the top-managers of the Brazilian Air Force Computer and Statistics directorate and of the BAF Materiel Command.

The objectives of this research are: (1) to estimate the total cost of ownership and operation of a networking solution for the Brazilian Air Force Materiel System (SISMA) using X.25 and using TCP/IP-Internet, and (2) by assessing security, performance, cost, and reliability issues, to determine the feasibility of using TCP/IP protocols and the Internet as a Virtual Private Network for the Brazilian Air Force.

Methodology

This research is divided into four major parts, to be performed in sequence. The first part consists of an overview of networking, the X.25 and TCP/IP protocols, and the characteristics of Virtual Private Networks. In addition, this research describes the current networking policy of the Brazilian Air Force. The objective is to understand the differences between the X.25 and TCP/IP protocols, and the cost element structure of the current BAF's network. Books, articles, IETF reports, "white

papers," CERT advisory reports, and Brazilian Air Force directives will be the principal references for this task.

The second part is an analysis of the current network model employed by the Brazilian Air Force for data communications. The objective is to become familiar with the characteristics of the network, and to analyze security, cost, and flexibility issues associated with it. Brazilian Air Force directives, contact with DIRINFE personnel, Department of Defense (DoD) directives, articles from specialized literature, and case studies will provide the most information for this work.

The main task in the third part is to develop the cost of operating and maintaining each of the network solutions. An alternative networking model based on the Internet as a backbone for carrying remote traffic using tunneling technology is presented. Security, performance, flexibility, and the cost structure of the proposed model are compared with the current Brazilian model. The data collected during the previous part of the research will be the basis for the definition of the most appropriate model in terms of the defined metrics of security, performance, cost, and flexibility.

The final part is the assessment of the feasibility of the proposed model, and the suggestion of the steps to implement the model.

Assumptions

Primarily, it is assumed that the benefits of the implementation of an organization-wide network are incontestable. It means that this research will not take into consideration the implicit questions regarding if the Brazilian Air Force needs full connectivity for its mission accomplishment. However, we can speculate that the implementation of a BAF network, independent of the model or protocols used, would be an excellent leverage to reduce costs, improve internal customer service, and improve the availability of weapons systems through a more streamline logistics system.

Although Virtual Private Networking is still an emerging technology, the literature about it is readily available. There are an increasing number of organizations - including the US DoD itself and those that need strong "military" security in data communications such as financial institutions and high-tech enterprises - currently using VPN to reduce networking costs. However, we can not assure that all the assumptions taken by this research will hold in a

military warfare context. For example, the majority of the cases covered deal with de facto-standard commercial applications. In the context of Information Warfare, one cannot assure that all the generally accepted commercial software and hardware are exempt from "backdoors," tamperproof modules, or any device that could compromise their reliability [22], and that "secret" mathematical treatment of academically and commercial apparently intractable equations used in cryptography are not developed by Intelligence Agencies around the world [23].

Scope and Limitations

Standards -- this research will try to avoid using any specific proprietary standards. However, given the dependence of networking on some kind of protocol, use of the Internet Engineering Task Force standards will be made where possible.

Peacetime/Wartime -- the scope of this research is the peacetime environment, although some concepts presented by this research can be extended to a wartime environment.

Commercial products -- it is assumed that current or future commercial products can be used to accomplish the implementation of the Virtual Private Network. However,

this research will try to select trusted commercial equipment as in observance to the DoD 5200.28-STD [41]. The research overviews commercially products available for international use in mid-1998, and makes a comparison between them.

Expected Results

The primary purpose of this research is to determine the feasibility of implementing a Virtual Private Network over the regular Internet backbone to transmit encrypted data between Brazilian Air Force's units. The feasibility study observes security and performance requirements, and compromise flexibility and cost issues. As a secondary product, the research addresses the current Brazilian Air Force's network status in terms of cost, security and vulnerability.

Significance of Research

The BAF Materiel Command is currently developing a major logistics information system called SILOMS (Logistics, Materiel, and Service Integrated System). The initial specifications of this system determine that every depot and operational unit should be connected to a central database.

In order to achieve it, X.25 links and/or satellite capability will be used. This research attempts to highlight the obsolescence of the X.25 protocol.

Security issues appear to be the principal concern in the use of TCP/IP protocols. This research studies the degree of security that can be achieved through the use of an alternative pipeline of data communications: the Internet. In addition, attention is drawn to security issues associated with the Brazilian Air Force networks, no matter the protocol or media used for transmission.

Another side result of this research is the estimation of the current network capability, security *status quo*, and costs of ownership, maintenance and operation. Therefore, the Brazilian Air Force could use the results of this research for future studies of network upgrades.

Summary and Research Organization

This thesis consists of five chapters. Chapter I presented an overview of the current BAF's communications network policies and the background of the research concerning the use of the Internet as a tool to leverage BAF's network capabilities. The chapter describes the four parts of the methodology, which approaches the features of

X.25 and TCP/IP protocols, issues of the current communications network used by BAF, and an alternative Internet-based model that uses VPN technology. The chapter also describes the assumptions, and the scope and limitations made regarding peacetime/wartime environment and the use of commercial products for implementing a VPN. Finally, the expected results of the research are defined as the determination of the feasibility of implementing a VPN over the regular Internet backbone for the transmission of encrypted data between BAF's units.

Chapter II consists of a literature review and presents an overview of X.25 and TCP/IP protocols, describes network security issues, presenting threats and usual "hacker" attacks to Internet-based networks as well their countermeasures. It also describes the features of VPNs that guarantee the establishment of secure channels over the Internet. The chapter also displays the current BAF's network infrastructure and the available Internet backbone in Brazilian territory. Finally, the review presents a cost breakdown method that will be used to calculate the costs of operating the current Brazilian Air Force network and the costs of operating the Internet-based model.

Chapter III consists of the research methodology of this thesis. The four major parts of the research design

are: (1) a review of networking security, (2) a review of a networking cost model and a study of its cost factors, (3) an analysis of the current Brazilian Public Network Infrastructure (that is, the Brazilian branch of the Internet Backbone), and (4) an analysis of data communications and security requirements for the BAF.

Chapter IV consists of the analysis of the costs involved in implementing the BAF's X.25 dedicated network. The analysis is presented in a breakdown structure and includes network access costs, hardware costs, software costs, maintenance costs and training and support costs. The chapter also discusses the implementation alternative VPN-based solutions. Based on this discussion, one of the alternatives is selected and its cost breakdown structure, following a pattern similar to the one used for implementing a X.25 network, is presented. Finally, the chapter displays a comparison of costs between the X.25-based solution and the VPN-based solution and calculates the payback period in which the VPN-based solution pays itself.

Chapter V draws some conclusions on the costs of implementing each one of the solutions, identifying their major cost factors. It also discuss four implications for the benefit of the Brazilian Air Force, which are (1) the implementation of SILOMS (BAF's Logistics, Materiel, and

Service Information Systems) and its relation to this research, (2) BAF's and the Internet context, (3)the security of information systems, and (4) Potential savings from adopting a VPN-based solution. Finally, the chapter adds some points for future research, such as expansion of this research to the context of Global Information Warfare, the use of prototype networks, and potential savings from a BAF wide implementation of a VPN.

II. Literature Review

Chapter Overview

The purpose of this chapter is to review the literature related to the X.25 protocol, the TCP/IP protocols suite, and Virtual Private Networking technologies. The review first describes some networking protocols, including the OSI Networking model, the low-level X.25 protocol, and the TCP/IP Internet protocols suite. This information is useful for understanding some concepts of Extranets and Virtual Private Networking, and for establishing the conceptual differences between the current and proposed models.

The literature review next studies those security concepts necessary to implement a Virtual Private Network, such as cryptography, network filtering (firewalls), and authentication. The review then examines the current framework of the Brazilian Internet Infrastructure and the Brazilian Air Force Materiel Command networking requirements.

The Extranet development life cycle (or Virtual Private Network life cycle development) is then introduced and the following items assessed: Requirements Definition, Analysis and Design, Prototyping, Construction, Testing, Implementation, and Maintenance [24].

Finally, the literature review develops the costs of ownership of the current network, and the costs associated with the Extranet model. Security and flexibility issues of the two models are compared.

Networking Specifications and Protocols

The OSI and TCP/IP Networking Models

According to Washburn and Evans [25], networks (and any-to-any communications) deal with three distinct requirements: (a) the ability to move data anywhere in an organization with chosen reliability, security, and performance; (b) the correct interpretation of that data in a manner appropriate to the receiving equipment; and (c) display of the interpreted information in an acceptable form for user consumption.

The first requirement is the core for the implementation of a successful network. The second and third requirements are outside the scope of this research, given that they are most suited for application development.

In 1977, the International Organization for Standardization (ISO) began to develop a communication standard called Open Systems Interconnection (OSI). This architecture model features intercommunication and

interoperability across different manufacturers' computing architectures (open architecture).

The OSI reference model establishes the communications functions partitioned into a hierarchical set of layers. Each layer performs a related subset of the functions required to communicate with another system, relying on the next-lower layer to perform more primitive functions, and to conceal the details of those functions, as it provides services to the next-higher layer.

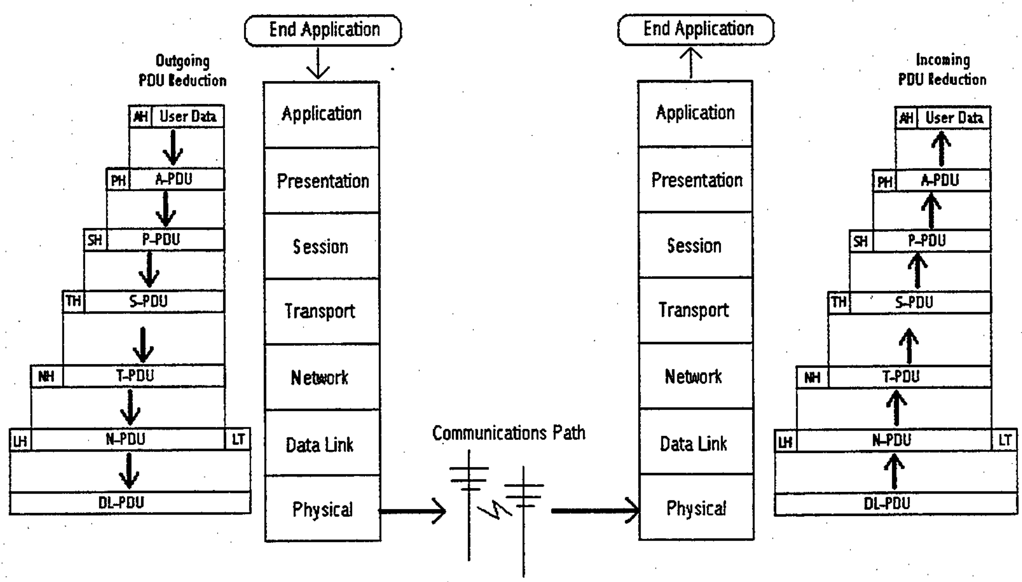


Figure 2.1 - The OSI Model [6]

Figure 2.1 represents the OSI layered environment: the lowest-level layer is represented by the physical layer, the highest-level layer is the application layer. Starting at

the application level, a header is attached to the data containing the necessary information to the next layer. This continue until layer 2 (data link), where both a header and a trailer are added. The unit, then called a frame, reaches the physical layer and is passed to the transmission medium. After being received by the target system, the process occurs in the reverse order, that is, as the data goes up, the headers and trail are removed in reverse order to which they were added.

One of the best known and most used implementation of the lower layers of the OSI model, the X.25 protocol standard - which specifies an interface between host system and a packet-switching network - was originally approved in 1976 and was last revised in 1993. An X.25 network provides an error-free, reliable, and flow-controlled point-to-point connection between two interfaces over a packet switched public data network. X.25 network connections are fixed physical connections, often referred as "dedicated connections." The physical packet switching network connection can be through a modem connection or a leased telephone line, via a digital connection (DDS), or via a special channel of an ISDN connection [6].

The basic technology of packet switching is fundamentally the same as it was in the early 1970s;

although some authors [10, 26, 27] consider packet switching as one of the few effective technologies for long-distance data communication. According to Stallings [10], one drawback on using the X.25 protocol is the considerable overhead associated with the packet switching. The overhead is justifiable when any of the links in the network presents a possibility of error. However, modern technologies such as Frame Relay and ATM (Asynchronous Transfer Mode) make the overhead of X.25 totally unnecessary, since they benefit from the use of low error digital facilities to provide faster, more reliable, and more accurate packet switching.

While ISO committees were developing the OSI protocols, the USA (notably the US Department of Defense) was developing an alternative set of protocols which became known as TCP/IP. These protocols became the US DoD standard in 1983 [77]. While the US government demanded TCP/IP protocols for every computer product - thereby ensuring every US government computer supplier provided it - private industry also boosted the use of TCP/IP protocols by developing new products based on this specification. With the release of the UNIX 4.2BSD Network Operational System by the Berkeley Software Distribution in 1983 for the public domain, the TCP/IP protocols emerged from the boundaries of the US DoD and the US university and research networks (ARPANet) [70, 77].

The differences between the OSI architecture and that of TCP/IP relate to the layers above the transport level and those at the network level. The TCP/IP protocols model deployed on the Internet consists of five layers instead of seven as in the OSI model. Two OSI layers, session and presentation, are not explicitly included on the TCP/IP specifications.

The five TCP/IP layers are: (1) physical layer - concerned with the network transmission medium (for example, coaxial, twisted-pair, fiber-optic cables) and its associated physical interfaces; (2) data-link layer - groups the bits being transmitted or received into frames, with the purpose of providing somewhat reliable delivery mechanism on the physical medium; (3) network layer - responsible for moving data between communicating end-points through routing tables - unless the sending and receiving hosts are on the same network, this job includes routing, determining the data along the best internetwork path; (4) transport layer - provides two types of service - the connectionless service UDP (User Datagram Protocol) and the connection-oriented, full-duplex service TCP (Transmission Control Protocol); and (5) application layer - entirely defined by the application developer. Hughes [26] shows the five-layer abstraction of the TCP/IP protocols in Figure 2.3. It is important to emphasize the difference between the services provided by

the transport layer: the TCP is a connection-oriented and full-duplex service, and it guarantees a reliable bi-directional stream of data re-transmitting lost packets, discarding duplicate data, and reordering packets out of sequence. This research focuses on the TCP transport service.

The format of a TCP data segment is represented in Figure 2.2:

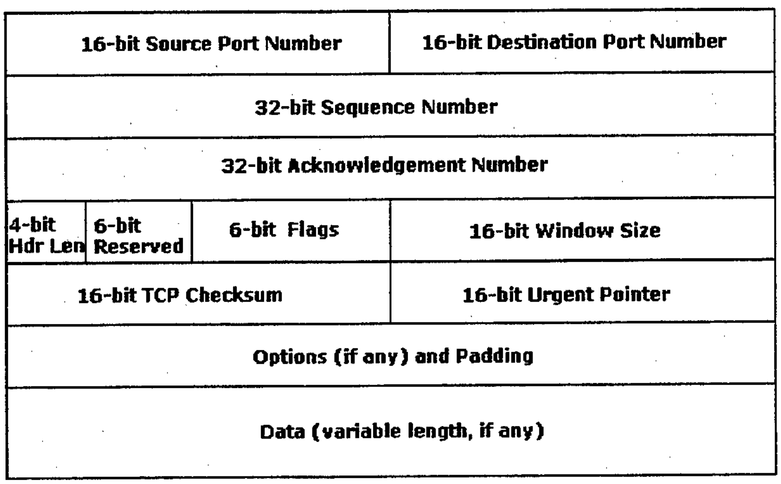


Figure 2.2 The TCP Data Segment [26]

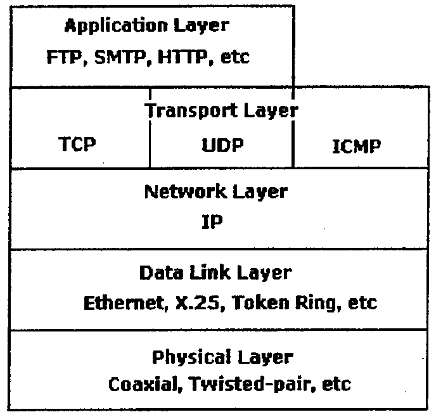


Figure 2.3 - TCP/IP Protocols Interfaces [26]

Security Concepts

Several authors [22, 26, 27, 28, 29, 30, 31] consider authentication, access control, integrity, confidentiality, and nonrepudiation the five "pillars" of network security. Authenticity assurance is related to the establishment of "identity proof." This is generally verified with the combination of something the user is, something the user knows, or something the user has. "What a user knows" can, for example, be an account identification and a password, for example. "What a user has" can be a hardware authentication device (much more like a physical key). Access Control deals with the access to some object or logical device based on the previous user identification. The access control problem, according to Hughes [26], is basically authorization, rights, and privileges. Integrity

relates to the reliability of the information contained in the document, i.e., the states between the time the message was sent by the sender and the time it was received. In that way, it deals with the risks of message alteration (added, removed, or modified) among the sender and receiver nodes by attackers situated in intermediate nodes. Confidentiality is related with the "privacy" of the messages (this concept can be much more broadened in terms of Information Warfare instead of being limited to personal privacy), i.e., avoiding release of the data content to third parties. Nonrepudiation, according to Garfinkel and Spafford [31], means that an individual cannot claim that the original message actually sent was not signed by him or her. Additionally, some authors [23, 27] include in this category the protection of network access to trusted users caused by unavailability due to "denial-of-service" attacks. Hughes [26] explored these security issues for each layer of the TCP/IP suite.

Threats at the Physical and Data Link Layers: according to the author, security at the physical and data link layers, is primarily concerned with access control, i.e., security of the physical transmission medium. In that way, electronic devices capable of network monitoring could be able to monitor (and perhaps act as a "man-in-the-middle") traffic between two nodes. Defining access control for

leased lines of third-party companies is indeed extremely difficult to implement. Consequently, the security threats for both solutions at this level - using X.25 and the Internet - are the same.

Threats at the Network Layer: relates to the layer's function of end-to-end datagram delivery. Some IP's vulnerabilities are: passive attacks (snooping or sniffing), message replay, message alteration, message delay and denial-of-service, address masquerading and address spoofing, unauthorized access, and routing attacks. Passive attacks (also called network eavesdropping) deal with the observation of network traffic without disturbing it. This can be accomplished by using software utilities originally designed for debugging application and network problems. According to CERT Advisory CA-94:01 [32], all systems that offer remote access through "rlogin" (remote login), telnet, and FTP are at risk. Sniffing software places a system's network interface into "promiscuous" mode, in which all the contents of network packets will be displayed (and even recorded) to the sniffing software. Encryption of datagram (or of its most important sections) is a viable solution, since the attacker will not be able to uncover the content of the datagram.

The message replay attack can be accomplished by snooping and then recording a conversation between two systems. At a later point, the recorded message is "play-backed" to the victim. The idea is to achieve the same result the first machine accomplished by exchanging with the victim, the same recorded message (including encrypted passwords). The only way to avoid such attack is through the use of encryption and one-time passwords (token passwords).

The message alteration attack deals with the integrity of the messages sent between trusted parties. Intermediary routers move a message from its source to its destination; however, those routers are able to modify some contents of the transmitted packets. An attacker positioned in one of the intermediary routers can modify the contents of a datagram, and also recalculate and update the header checksum. Encryption techniques such as digital signature can be used to assure data integrity.

Message Delay is caused when datagrams are retained or under different conditions, made undeliverable for an unwarranted period of time. Denial-of-Service causes datagrams to be rejected before final delivery, effectively blocking the communication channel and making the target host inoperable.

Concerning authentication issues at the Network Level, address masquerading and address spoofing are the major exposures. Address masquerading occurs when the attacker machine network interface is configured with an address intended for another system. It can be easily accomplished in an Ethernet network by changing the identification settings of network cards. In the TCP/IP environment, some higher-level protocols (such as the Sun's Network File System [26]) are an easy target for this kind of attack. Address Spoofing, also called TCP sequence number attack [33], explores a known flaw in many TCP/IP implementations. Morris [34] first issued a publication addressing spoofing in 1985. While address masquerading is generally restricted to local networks, address spoofing is possible across the Internet. This type of attack exploits the "three-way TCP handshake"[1] that establishes a reliable connection between host and remote. Fortunately, there are several defenses against address spoofing. The first method is to avoid reliance on address-based authentication (through the IP address) and trust mechanisms based only on passwords. The second approach is to use screening routers - a device

[1] TCP/IP three-way-handshake process - Host A wishes to establish a connection to Host B. Host A sends a solitary packet to Host B with the synchronize bit (SYN) set will announcing the new connection and an Initial Sequence Number (ISN) which allow tracking of packets sent between hosts. Host B responds to the request by sending a packet with the synchronize bit set (SYN) and acknowledgment (ACK) bit set in the packet back to the calling host.

capable of filtering network packets based on configurable rules. Screening routers can be configured to block incoming datagrams with a source address belonging to the internal network (inbound attack) and block outgoing datagrams with a source address from an external network (outbound attack).

The Internet was primarily designed to be an "open architecture," and to allow completely unrestricted connectivity. However, there are several techniques to restrict access to sensitive information by computers and networks connected to the Internet. Two techniques will permit the implementation of access control: packet filters and firewalls. Packet filters operate at the Network and Transport Layers, and Firewalls operate at the Network, Transport, and Application Layers.

Newmann et al. [35] made a comparison between commercially available Firewalls in March 1997, and examined four attack scenarios in order to assess the vulnerabilities of each firewall. Lipschutz [36, 37] also evaluated security, ease of use, performance, and ability of Windows NT firewalls to handle distributed objects technologies such as CORBA and DCOM. According to Ahuja [38], the grades of security provided by firewalls can be established as shown in the Figure 2.4:

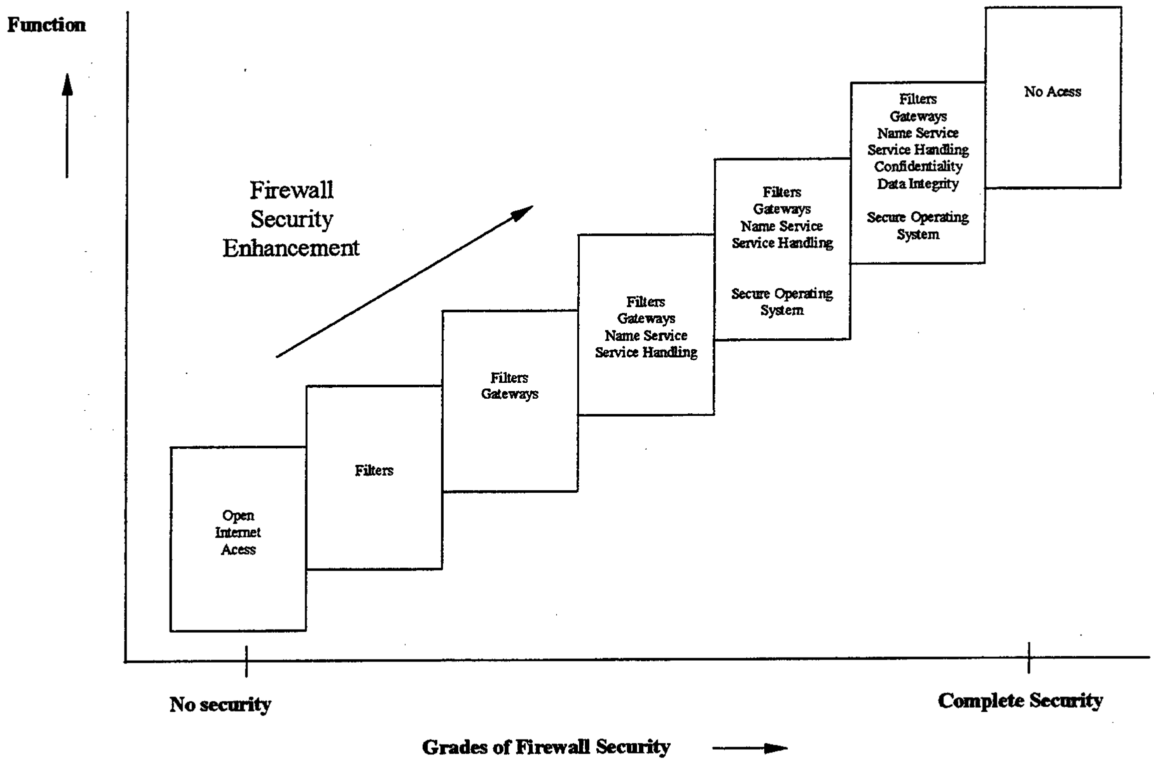


Figure 2.4 - Networking Security levels [28]

Routing attacks exploit the IP's source routing feature. The TCP/IP specifications establish that routes between two nodes should be dynamically determined based on factors such as link availability, distance, and speed between router "hops." Attackers can attempt to alter route rules by including his/her computer in the source route. Theoretically, after a host begins routing packets to an address chosen by the attacker, every datagram goes through the altered route path (including the attacker's machine). Unfortunately, there are not many ways to avoid this threat. However, one potential solution is the use of logging

devices with strict rules for routing protocols as discussed by Hare [26].

<u>Threats at the Transport Layer</u>: TCP and UDP datagrams can be easily replayed or altered, and there is no guarantee of authenticity at the network layer. Therefore, attacks that can take over an open connection or login from a remote host for its own control are known as hijacking attacks. This attack is generally used in conjunction with IP spoofing techniques, and, if successful, can possibly lead to root access over the targeted system. According to CERT Advisory report CA-95:01 [39], "current intruder activity in spoofing source IP addresses can lead to unauthorized remote root access to systems [even] behind a filtering-router firewall." Attackers possessing root accounts can then modify and delete files on the system, and therefore compromise overall system security [72]. Unfortunately, although there are many ways to detect hijacking attacks, there is no specific way to prevent it.

<u>Threats at the Application Layer</u>: a variety of weaknesses can be exploited at the application level. These weaknesses are generally related to inappropriate implementation of security policies. Inexperienced or untrained users accidentally publicizing their passwords, weak passwords, "social-engineering," virii and trojans, and

physical access to terminals (ingress) are the most common threats at this level.

Network Security: part of the problem of Internet security is related to the fact that the TCP/IP protocols were designed to permit interoperability and interconnectivity, not impenetrability [21]. This study has discussed some of the most common types of attacks and threats for Internet security. Indeed, there are an extensive literature dedicated to the topic of network security, but Tate [21] has shown that the real challenge of network security is developing an integrated security concept, and that security is a direct function of the cost of the assets being protected. The author included as critical integration issues: Virtual Private Networking, Firewalls, Network Security Protocols, Encryption, Security Tools, Access Control, Proxy Agents, Authentication, Intrusion detection (logging), and Security management.

Schwartau [23] classified levels of Information Warfare in three categories: Class 1 - Personal Information Warfare; Class 2 - Corporate Information Warfare; and Class 3 - Global Information Warfare. According to the author, the last category, which deals with Information Warfare between countries or between a country and an organization, is the ultimate level of Information Warfare. He commented that at

this level, Information Warfare is accomplished by an "Information Army" composed of 11 types of "skills": mappers, crackers, sniffers, readers, software development group, moles, analysts, manufacturing group, software distribution group, and public relations group.

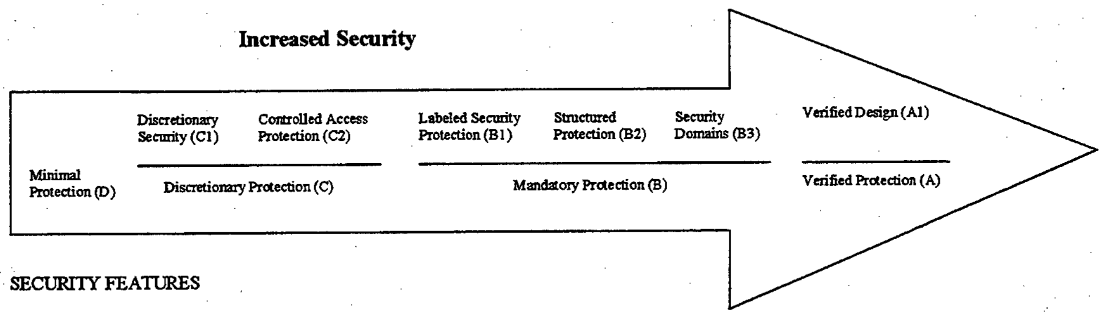
GAO Report AIMD-96-84 [1] recommended to the US Secretary of Defense that a more effective information systems security programs should include:

> Improving security policies and procedures, increasing user awareness and accountability, setting minimum standards for ensuring that system and network security personnel have sufficient time and training to properly do their jobs, implementing more proactive technical protection and monitoring systems, and evaluating Defense's incident response capability.

In addition, a recent security audit performed by US federal investigators (specifically, the General Accounting Office) concluded that the US Department of State and Federal Aviation Administration is "wide open and vulnerable to attack" [40]. The auditors' findings included "easy penetration to unclassified State Department systems by exploiting lax physical security, dial-up connections, and easily guessed passwords;" lack of intrusion detection devices; and "lack of a central point for overseeing and coordinating computer security."

In order to deal with security standardization, the United States Department of Defense developed several levels of security standards in DoD Directive 5200.28-STD "Trusted Computer Standards Evaluation Criteria," [41] also known as the "Orange Book." The directive has remained unchanged since it became the DoD standard for network security in 1985. According to this directive, these levels of security describe different types of physical security, user authentication, trust levels, and user applications. The levels of security are classified as Level D1, Level C1, Level C2, Level B1, Level B2, Level B3, and Level A (as shown by Figure 2.5). Level A is currently the highest level of security with the narrowest level of design, control, and verification process, while Level D1 is the lowest form of security [28].

The classification of the Trusted Computer Standards is based on four constructs: security policy, accountability, assurance, and documentation. This study deals with networking systems that falls into "C" category, and in the "C2" subcategory. C2 Class is considered as the minimum class for information systems that deals with sensitive information [38]. It is assumed that the security desired for this study requires identification, authentication, access control, and auditing on an individual basis, as in the C2 class.



SECURITY FEATURES

Minimal Protection (D)

- No features

Discretionary Protection (C)

- Identification and Authentication
- Discretionary Access Controls
- Object Reuse
- Audit
- Security Testing
- System Architecture (Process Isolation)

Mandatory Protection (B)

- Labels
- Mandatory Access Controls
- Design Specification and Verification
- Covert Channel Analysis
- Trusted Facility Management
- Configuration Management
- Security Testing (Penetration Testing)
- System Architecture (Software Engineering)
- Trusted Recovery

Verified Protection (A)

- Design Specification and Verification (Formal Verification)
- Trusted Distribution
- Covert Channel Analysis (Formal Covert Channel Analysis)

Figure 2.5 - Classification of Security Components based on the DoD Evaluation Criteria [26, 41]

A C2-Class computer system should be able to provide Discretionary Access Control (DAC), Accountability (Identification, Authentication, and Audit), and Assurance (System Architecture and System Testing).It is clear that absolute protection of Defense information is neither practical nor affordable [1]. Risk management, given the systems requirements, is the best way to ensure computer security. Tradeoffs between the value and sensitivity of the information, the possible threats, and the cost of protecting it should be taken into account when designing a computer system.

GAO [1] rates the following security activities as the most important for implementing an appropriate and well established networking policy:

1. Clear and consistent information security policies and procedures;
2. Vulnerability assessments to identify security weaknesses at individual Defense installations;
3. Mandatory correction of identified network/system security weaknesses;
4. Mandatory reporting of attacks to help better identify and communicate vulnerabilities and needed corrective actions;
5. Damage assessments to reestablish the integrity of the information compromised by an attacker;
6. Awareness training to ensure that computer users understand the security risks associated with networked computers and practice good security;
7. Assurance that network managers and system administrators have sufficient time and training to do their jobs;
8. Prudent use of firewalls, smart cards, and other technical solutions, and
9. An incident response capability to aggressively detect and react to attacks and track and prosecute attackers.

According to the GAO [1], policy reviews are the number one actions that should be taken to create a consistent and feasible system security policy. A strong set of security policies and procedures is the main component of a reasonable network security system. Another vital point suggested by many authors [1, 24, 29, 30, 31, 42] is to maintain security personnel, who are well trained and well informed about the breakthroughs in network security issues, new exploits, and software bugs found. Many authors also suggested the creation of a "response team" for detection and reaction against attacks and establishment of overall network security policies [73, 74, 75, 76].

Hundley et al. [2] and others [73, 74, 75, 76] have discussed some protective techniques and strategies that have an important role in networking security. They are listed as firewall implementation, improved access control, more secure software and operating systems (elimination of software bugs and exploits in the coding phase), encrypted communications, encrypted files, improved capabilities to detect penetrations (auditing trail), active counteractions, and software agents.

In studying the feasibility of using the TCP/IP protocols and the Internet as the media for Brazilian Air Force's data traffic, apart from the policy and procedural

issues, several security principles should be taken into account. These key components are described by some authors as Authentication and Access Control, Cryptography and Firewalls, and System Integrity and Auditing, when dealing with a C2 Class information system [76].

The key to a secure extranet, according to Pfaffenberger [27], is based on the use of cryptography. According to Loshin [11], "extranet [and also Internet] security relies on standard-based authentication, encryption, and digital signatures."

"Encryption ensures that network elements cannot eavesdrop on the communications by "scrambling" the data," according to Microsoft's Security Overview [43]. However, a more formal definition of cryptography and encryption of data can be obtained on "Cryptography" [44:1]:

> The fundamental objective of cryptography is to enable two people, usually referred to as Alice and Bob, to communicate over an insecure channel in such a way that an opponent, Oscar, cannot understand what is being said. This channel could be a telephone line or computer network, for example.

Figure 2.6 presents the elements of a cryptosystem and the role of "Alice," "Bob," and "Oscar."

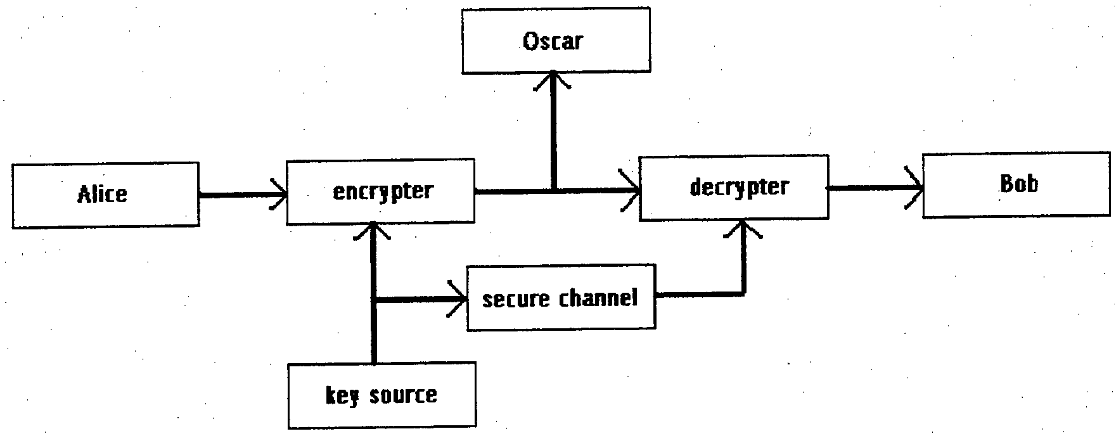


Figure 2.6 - Elements of a Cryptosystem [44]

In that way, cryptography provides an explicit mechanism to provide data privacy of information flowing through an insecure channel like the Internet [45]. Cryptography also permits signature schemes to be employed in network communications. "Digital signatures" employs one-way mathematical function (also known as hash function) to map large values into smaller, verifiable values called message digests. Message digests are then encrypted using the sender's private key. The final message consists of the encryption of the original message appended with the encrypted message digest.

Encryption algorithms are divided in two categories: private (symmetric) and public-key cryptosystems [46, 47]. A private key cryptosystem employs the same secret key for encryption and for decryption, while public key

cryptosystems employ a "pair of mathematically related keys: a private key that is kept secret within the system, and a public key that can be made known to the public" [45]. Drawbacks associated with private key cryptosystems include difficult of transmitting the key through a secure channel (in that way, direct face-to-face negotiation is the perfect solution to this drawback) and the necessity to change keys periodically. However, private key cryptosystems are very fast.

Some symmetric encryption algorithms are DES, 3-DES, RC2, RC4, RC5, and IDEA. DES (Data Encryption Standard) was developed by IBM in 1976, and became a U.S. Government standard in 1977. DES uses a 56-bit key and is considered secure only for "nonvital transactions." Some authors argue that the DES algorithm would probably contain a backdoor for easy eavesdropping, however, no technical proof has been made [22, 23, 44]. In fact, a group called the Electronic Frontier Foundation (EFF) has mounted a specialized computer array capable of breaking a 56-bit DES encryption key in less than 56 hours, at cost of $ 100,000, using an algorithm different from an exhaustive key search [48].

3-DES is nothing more than encrypting a message three times using the basic DES algorithm. This method offers a higher degree of protection, supposing the absence of

backdoors. RC2, RC4, and RC5 are proprietary algorithms from RSA Data Security, and their use requires licensing. RC2, RC4, and RC5 are considerably faster than DES, and can provide higher security given the larger key-length used to encrypt the messages. These algorithms operates with different key sizes from 0 to 2048 bits. The IDEA (International Data Encryption Algorithm) was developed in Europe by the Swiss Federal Institute of Technology. It is a block cipher that uses a 128 bit key.

Regarding public-key algorithms, the *de facto* standard is the RSA's patented RSA algorithm. The RSA algorithm has no limit of key length, although the most common key lengths used are 512, 1024 and 2048 bits. It relies on the difficulty of factoring an extremely large number composed of two large prime numbers. One drawback of RSA encryption is that it is 100 times slower than DES (when implemented by software).

Another public-key algorithm is the Diffie-Hellman (DH) implementation. It is very similar to RSA, including speed and no boundary of key-length, although it uses a different concept - it relies on the difficulty of solving discrete logarithms in a finite field. Appendix D presents some symmetric algorithms and one-way hash functions currently available.

According to Blaze et al. [8] and Schneier [49], recommended key-lengths for cryptographic algorithms depends on the time frame needed to maintain secrecy and the power of the attacker. Dealing with today's computer power and government's budgets, the minimal key length used for encryption of sensitive information should be 1536 bits. Extrapolating to the computer power available in the year 2015, the minimal key length should be 2048 bits [49].

Current VPN solutions employ private key encryption algorithms and public-key algorithms with different key lengths. Given that public-key algorithms are generally far slower than symmetric algorithms, both algorithms are used to encrypt data. The technique consists of encrypting the raw data using a symmetric algorithm and some random key, and encrypting the random key using some public-key algorithm. DES, 3-DES, and RC4 are the most common symmetric algorithms, while RSA and Diffie-Hellman are used as public-key encryption algorithms. Using a combination of digital signature schemes, key distribution system, and a symmetric key encryption system, an encrypted VPN session can be established between two computers, assuring data privacy, data authenticity, and data integrity.

Concerning user authentication, some of the most common schemes include the well known operating system

userid/password combination, S/Key (one time, or token) passwords, RADIUS authentication scheme, and strong two-factor token-based scheme [45].

Virtual Private Network solutions employ several techniques to tunnel encrypted data through an insecure channel, in this case, the Internet. Four transmission modes are presented in [50]: "In Place Transmission Mode, Transport Mode, Encrypted Tunnel Mode, and Non-encrypted Tunnel Mode." In Place Transmission Mode operates by encrypting only the original data (payload) of each packet; however, the packet size is not affected. Transport Mode operates by encrypting data and by changing the packet size according to the encryption mechanism. Encrypted Tunnel Mode encrypts both IP header and the original data, and the result is containerized in a new IP packet with a mapping to the VPN ending points. Non-encrypted Tunnel Mode operates without encryption. The data is only encapsulated in IP packets, but in clear text.

Encrypted Tunnel Mode provides the greater overall data privacy, according to several authors [21]. Details of this technique can be found in the Figure 2.7.

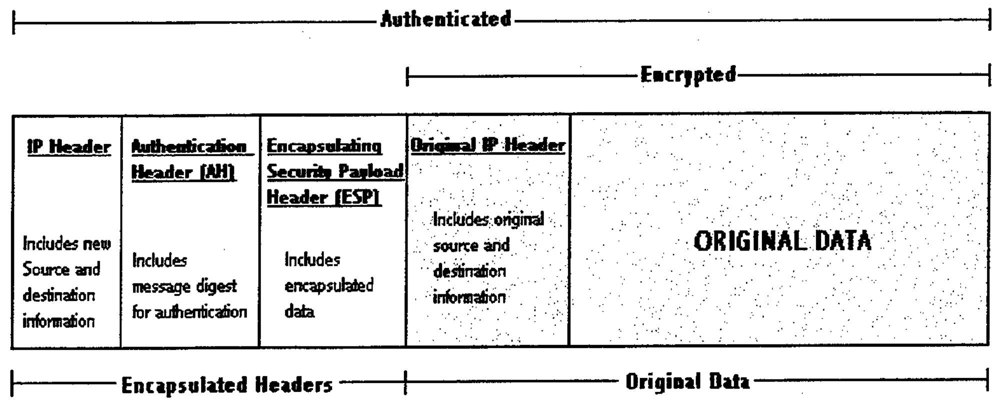


Figure 2.7 - Packet Tunneling [50]

An important question to be analyzed is where the encryption is actually being accomplished by the diverse techniques. Some techniques use encryption of data at the application level, while others at the IP stack (network level).

IPSec utilizes encryption at the network level. This technique seems more appropriate not only for privacy and authenticity but also for masquerading the actual destination address of the packets being transmitted.

The Brazilian Internet Infrastructure

The Internet is a relatively recent phenomenon in Brazil. Given that the Brazilian telecommunications sector was primarily monopolistic, the Brazilian Government

proposed the creation in 1988 of a Brazilian Internet committee to study the implementation of a national network infrastructure. This network infrastructure was called RENPAC ("Rede Nacional de Pacotes"), and was effectively implemented on September 1989. Initially, the network was composed of dedicated links with speeds ranging from 9.6 to 64 Kbps. Today, the Brazilian Internet Backbone is composed of links of 2 Mbps between the main Brazilian cities and 64 KBPS to 128 Kbps in the other cities [51, 52]. Predictions [42] suggested an expansion in the capacity of the backbone, as occurred in the original Internet in the United States, as shown in the Figure 2.8 and Figure 2.9.

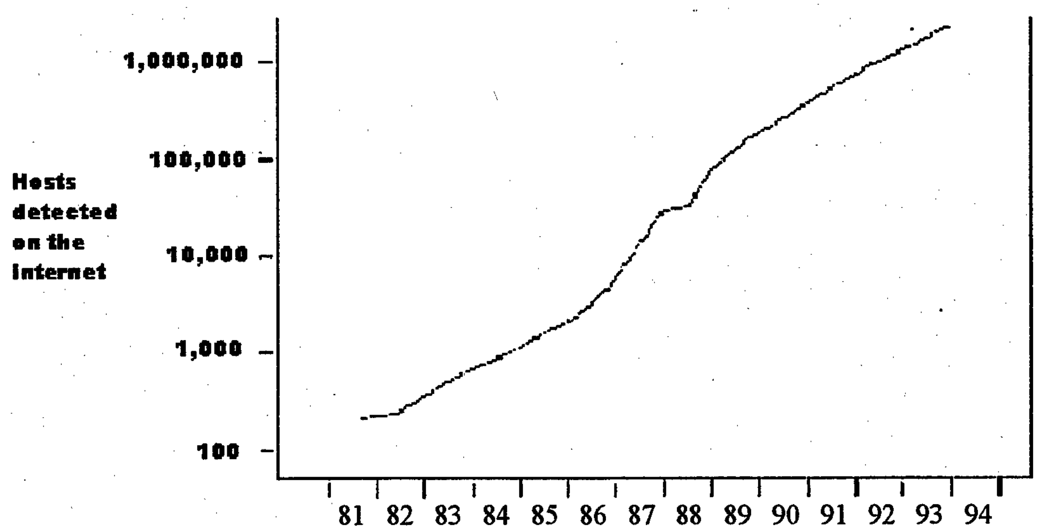


Figure 2.8 - Internet Growth during the period 1981 to 1995 [31]

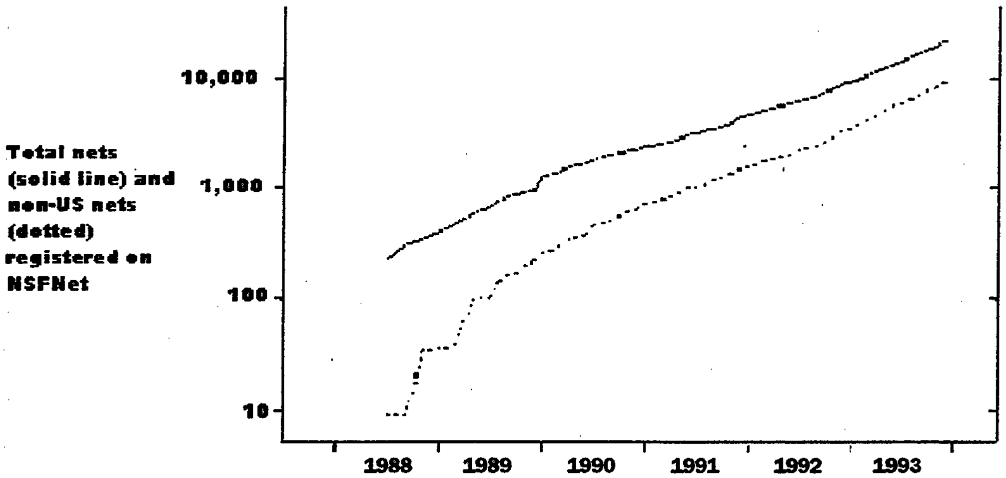


Figure 2.9 - Total Number of Networks registered on the Internet [31]

The expansion of the public network (backbone) will probably be supported by the commercial development of the Internet, given that all formerly public carriers are being privatized, and that there is no short term plan for BAF-owned cabling. If the same Internet "explosion" trend that has happened in the entire world reaches Brazil, we can expect to see substantial improvement in the Brazilian Internet backbone in the next few years. Maybe more connections between key points and increase on links capacity will be the first notable improvements.

The current Brazilian Internet backbone is shown in the Figure 2.10.

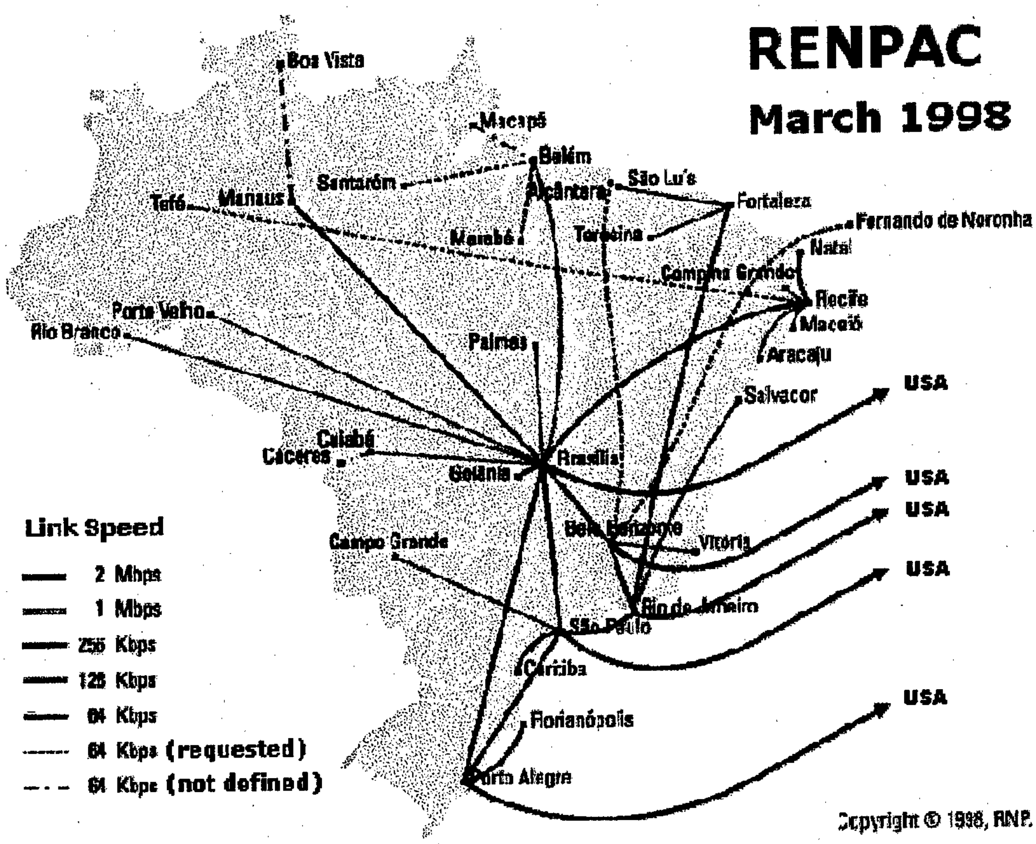


Figure 2.10 – Brazilian Internet Backbone as in March 1998 [51]

One problem of implementing a Virtual Private Network in Brazil is the lack of an Internet Service Provider (ISP) that covers all the Brazilian territory. In general, the Brazilian access to the Internet backbone is made through small ISP's that unfortunately do not offer the same level of customer service, reliability, and low costs as Global

Intranet Providers such as Equant, IBM, Infonet, CompuServe, and many others [53]. Therefore, in designing the Virtual Private Network, a solution relying on ISP's for transmission of tunneled data is not feasible.

The Brazilian Air Force's Network Infrastructure

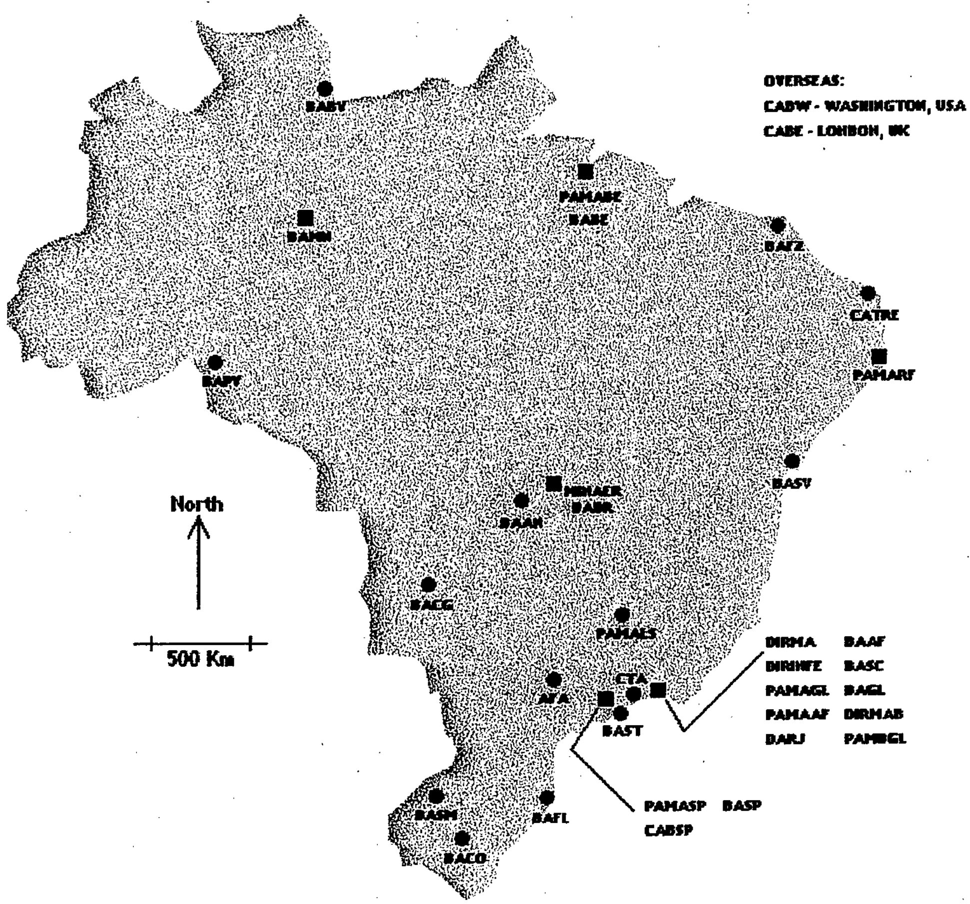


Figure 2.11 - Brazilian Air Force Materiel System Units

The Brazilian Air Force Materiel System locations are shown in Figure 2.11.

The BAF's Materiel Command Structure is composed of five depots and twenty operational bases. Depots are classified as level A (higher level of strategic importance), level B, and level C. Level A depots include Galeão Aeronautical Depot (PAMA-GL), Afonsos Aeronautical Depot (PAMA-AF), and São Paulo Aeronautical Depot (PAMA-SP). Level B depots include Lagoa Santa Aeronautical Depot (PAMA-LS) and Recife Aeronautical Depot (PAMA-RF). There is only one level C depot, the Belém Aeronautical Depot (PAMA-BE). There is also a depot specialized in armaments and weapons (PAMB-GL), that can be considered a level B depot.

Twenty operational bases, including the BAF's Academy (AFA) and Tactical Aerial Command (CATRE), are spread through the Brazilian territory. Three high level commands (DIRMA, DIRMAB, and DIRINFE) and the BAF headquarters (MINAER) are included in the model. Additionally, three BAF procurement commissions - one in the Brazilian territory (CABSP), one in Washington-USA (CABW), and one in London-UK (CABL) - and the Brazilian shipment unit (DARJ) are included in the model. Additionally, the Aerospace Research Center (CTA) internet link is included in the model.

Currently, the Brazilian Air Force employs several X.25 links between the units in São Paulo (BASP, PAMASP), Rio Grande do Sul (BACO), Brasília (MINAER), Pernambuco (BARF,

PAMARF), Pará (PAMABE and BABE), Amazonas (BAMN), and Rio de Janeiro (BAGL, PAMAGL) to the concentrator at Rio de Janeiro (DIRINFE). The Brazilian Air Force currently has a project of connecting all BAF's operational bases to this computer network in order to achieve a greater integration of information systems in use [3]. Users of this network will be the DAC (Civil Aviation Department), DIRMA (Materiel Command), DIRINT (Administration Command), DIRSA (Healthcare Command), DIRENG (Engineering Command), and all units of the COMGAP (Support Headquarters). The application systems which has the mission of managing maintenance activities and logistics support is called SILOMS (Integrated System of Logistics and Services).

Networking Cost Breakdown

Several authors studying the Return on Investment (ROI) of implementing Extranets and Intranets reported that typical ROI can reach over 1000% and payback periods ranging from six to twelve weeks [17, 19, 54, 55].

Bayles [24] suggested that building, implementing, and maintaining an extranet involves allocating infrastructure costs, direct project costs, and distributed costs. According to him, infrastructure costs are associated with telecommunications lines and equipment, direct project costs

are associated with maintaining and operating servers, building web-services (HTML documents, etc), and distributed costs are associated with maintaining the distributed links. Campbell [54] reported that "the cost of hardware and software was far less significant than the cost of personnel," and continues, "personnel costs fell into two distinct categories: the one-time cost of application development, and the ongoing costs associated with supporting the system and maintaining a steady flow of information content."

The following breakdown cost framework is suggested by Bayles [24]: Hardware Costs, Software Costs, Internet Connection Costs, Server/Site Hosting Costs, Security Costs, Development Costs, Training Costs, Maintenance Costs, Support Costs, Management Costs, and Depreciation Costs.

Hardware Costs involve costs to acquire and maintain servers, routers, hubs, switches, gateways, and workstations. In the case of traditional private networks using the X.25 protocol, cost of X.25 adapters, computer cards, and modem banks should be included in this category. Software costs involves costs of the server operational system and Internet server software, database software, mailing software, and telecommunications software.

Internet Connection costs are those costs incurred in using leased telecommunications lines (installation and monthly charge) and ISP installation and monthly fees, or the contract value in the case of contracting a single ISP to provide all Internet access. Server/Site Hosting Costs are those related to site/server maintenance and Web hosting (in the case of Web-developed content).

Security costs involve those costs of buying firewall and packet filtering devices and software, security audit tools, RSA Certificates, additional routers and gateway machines, and security staffing costs. Training costs are accounted for employee and staff training in using Internet-based network solutions and ongoing training. Maintenance costs are basically related to server backup labor and equipment, hardware servicing, and software upgrades. Support costs is included as an additional cost category, and it includes bug tracking system, Air Force's Computer Emergency Response Team implementation and operation, and system administrator's salaries. Depreciation costs include annual depreciation of hardware and software. The complete cost breakdown structure is presented in Appendix C.

Web-pages design and content development costs are not included in the model, since we considered those costs as

development costs of the front-end application being developed to the maintenance system (SILOMS).

Summary

This chapter presents a literature review describing the beginnings of the OSI model in the mid 1970s, and introducing the X.25 protocol as the most used implementation in the OSI model's lower layers. Regarding packet switching, the chapter emphasizes that the X.25 protocol, yet reliable and error-free, displays a weighty overhead in comparison to modern technologies (such as Frame Relay and ATM). Next, the chapter describes the role of the US DoD in the conception of the TCP/IP protocols suite and the establishment of the ARPANet, and displays the basic mechanism of these protocols.

Regarding security, the chapter evaluates threats and "hacker" attacks according to the layers of X.25 protocol and TCP/IP protocols suite, that is: (1) threats at the physical and the data link layers, in which the intruder is able to act as a "middle man" and monitor traffic between two nodes; (2) threats at network layer, which lists attacks such as "snooping," "spoofing," message alteration, message delay, message replay, denial of service, among others; (3)

threats at the transport layer, also known as hijacking attacks, in which the attacker replays or alters TCP and UDP datagrams; (4) threats at the application layer, which are usually related to the "modus operandi" of users (passwords publicized by accident, weak passwords, etc). Moreover, The chapter explains the mechanism of encryption, showing its two basic categories (private cryptosystems and public-key cryptosystems) and discussing encryption techniques adopted by VPNs.

The chapter also examines the brazilian internet infrastructure and emphasizes the lack of high level customer service and reliability. However, the chapter foresees that the Internet "boom" will reach Brazil very soon, which will help to overcome these problems. In addition, a description of all the units that form the BAF's Material System is presented.

Finally, the chapter discusses breakdown structures used to estimate costs of implementing networks, presents a brief consideration on what type of costs are to be included in each alternative (X.25 protocol and TCP/IP protocols suite) and states that, generally, the investments in the implementation can be recovered be recovered in periods from six to twelve weeks.

III. Methodology

Chapter Overview

The literature review illustrates selected aspects of cost and security related to the implementation of a Virtual Private Network. The public sector is leading the use of VPNs in order to reduce costs of networking, and some studies pointed out that more than US$ 100,000 [15] can be saved per year in substituting dedicated networks to Internet-based solutions in the commercial sector. We established the feasibility framework in terms of cost, security, and flexibility in using the concept of Virtual Private Networking over the "public" Internet backbone to transport data between the Brazilian Air Force's bases, depots, and Commands. In the context of the military, the use of VPN is not limited to peacetime operations, but also for wartime. However, special requirements in the case of wartime should be evaluated to the context of Information Warfare. Technology to implement VPNs is now available in order to use "military" graded security technologies such as strong encryption and authentication in order to achieve higher levels of computer security. Perhaps the most important factors to enhance communications capability and share information using the Internet is to update policies

that govern computer security, and increase security training for systems and network administrators. According to the GAO report AIMD-96-84 [1], "security breaches cost DoD hundreds of millions of dollars annually," and, "the potential for catastrophic damage is great." However, according to the same report, the feasible solutions to improve protection of Defense information would be the use of firewalls, smart cards, and network monitoring systems. The report also commented that "the success of these measures depends on whether Defense implements them [technical solutions] in tandem with better policy and personnel solutions." This thesis also studies DoD's "lessons-learned," necessary policy changes, and techniques that can be effectively used in order to protect Brazilian defense information infrastructure. This chapter describes the methodology used for the research, including research objectives, research design and implementation, expected results, and scope and limitations.

Research Objectives

Brazil has the fourth largest territory in the world (exceeded only by Russia, Canada, and China), if counting only the continuous surface, or fifth (behind Russia, Canada, China, and United States), if considering the entire

United States territory (including Alaska). With more than 8-million square kilometers of surface, north-south distance of 4,320 Km. and east-west of 4,395 Km., the Brazilian Air Force has to cover enormous distances in order to successfully accomplish the mission of maintaining the Brazilian aerospace power. The Brazilian Air Force operates with five depots of which three are concentrated in the Southeast portion of the Brazilian territory. However, several bases are installed in regions of difficult access, such as in the Amazonian rain forest, where the distance between points of presence can reach several thousand kilometers. Luckily, the Brazilian public Telecommunications Company (Embratel) maintains either physical or satellite links between these points. Currently, the Brazilian Air Force uses this capability to connect the "main" infrastructure of depots and bases with links of 9,600 bps. However, remote points of presence virtually do not have any data communications capability. Consequently, this study deals with the lack of computer communications resources faced by the Brazilian Air Force. This problem is due mainly to the large distances between Brazilian Air Force's points of presence (depots, bases, and Commands), to the lack of an integrated network infrastructure, and to the high costs and lack of security

involved in the use of rented or leased communications cables.

Therefore, the objectives of this research are:

1) to determine how the Brazilian Air Force can use the Internet (the Brazilian public network infrastructure) to establish unclassified data communications between points of presence;

2) to estimate the cost associated with the implementation and operation of a Brazilian Air Force Virtual Private Network over the Internet to integrate the BAF's logistics system, and compare with the current solution of using dedicated lines using the X.25 protocol;

3) to assess security issues related to the use of the Internet and the TCP/IP suite protocol.

Research Design and Implementation

This research is divided into four major parts, to be performed in sequence.

Review of Networking Security. The first part consists of the overview of networking issues, the Internet TCP/IP protocols model, and facets involved with Internet security.

Primarily, the objective is to study basic security requirements of data networks, and to understand the

technical specifications of the TCP/IP model. Secondly, based on the previous knowledge of the technical specifications of the Internet model, the study deals with the identification of the threats and risks involved on connecting computers to the Internet. After that, we study the possible solutions, such as cryptography, packet filtering, and firewalls, for the identified threats in order to include in the Virtual Private Network solution.

Security requirements are based on documents of the U.S. Department of Defense. The effort was conducted collecting several books of networking protocols and security, articles about encryption techniques, VPNs, hacker attacks and exploits - including consulting well known hacker sites, magazines, discussion groups, and mailing lists; and CERT's (Computer Emergency Recovery Team) reports on the subject of network and Internet security.

Review of a Networking Cost Model. The second part consists of the study of the cost factors involved in setting up a data communications network. The objective is to comprehend the cost elements and structure of implementing, setting up, and maintaining a Virtual Private Network and a dedicated communications network, and to choose a method to compute the ROI (Return on Investment) of

both solutions. The books "Extranets - Building the Business to Business Web," by Bayles [24] and "Building a Strategic Network," by Pfaffenberger [27], serves as the starting points. These books provide a framework of the infrastructure, direct, and distributed costs involved in the designing, building, and maintaining an extranet solution. The next step is to search for previous cases of Virtual Private Network implementations, and to assess costs and security issues related to it. Also, price lists of carriers, ISPs, and hardware manufacturers are used in order to establish the costs.

Analysis of the Brazilian Public Network Infrastructure. The objective of the third part is to make an analysis of the current Brazilian Network Public Infrastructure (or the "Brazilian" Internet backbone).

The primary source of research is based on the documents found on the Brazilian Telecommunications Company (Embratel) web-site regarding the Brazilian Internet backbone and Brazilian Air Force directives and instructions. Internet Web-based searches and e-mail contact with carrier companies and several Internet Service Providers are made in order to establish costs of Internet access.

Analysis of the BAF Data Communications and Security Requirements. The fourth part is an analysis of the current BAF's logistics system demand for data communications capability. The objective is to identify the points of presence involved in the logistics system in order to determine a feasible network topology and make an estimation of the network load demanded for each point, and the basis of 9,600 bps currently in use is based as the minimum throughput for any individual site.

The estimation of network traffic is made on arbitrarily assigned categories of the points of presence according to the logistics hierarchy. The authors assumed a client-server topology and servers located on command sites.

This part of the research will collect the number of requirements that was made for logistics support on 1997 for the PAMASP depot as the ceiling of the number of requisitions. Brazilian Air Force directives, units' annual work program, relative physical localization, and the available public network topology will provide the most information for this work.

Scope and Limitations

Hardware and Software - although this research deals specifically with the implementation of a Virtual Private Network using commercially available hardware and software, the scope of the analysis made by the research is not applicable just for a determined commercial solution. The hardware platforms are considered as Windows and Unix servers, and Windows clients. Software implementations specifically for logistics applications are not taken into account.

Currency - the values will be shown in American dollars. Values collected in Reais (Brazilian currency) will be converted to American dollars by the conversion factor of 1 American dollar = 1.00 Brazilian Reais.

Internet Protocol IPv4 and IPv6 -- since there are no signals (results, implications) of the effective and immediate commercial implementation of the "new" Internet protocol (IPv6 or IP-Next Generation), we assumed that the existing IPv4 Internet protocol would be used. In addition, the new Internet protocol will have back-compatibility with the old protocol. However, our specifications included for the possible solutions take into consideration the implementation of IPSEC as mandatory.

Disclaimer - since this research has not been officially sponsored by any BAF organization, the data here disclosed will not be endorsed by the Brazilian Air Force and may not precisely correspond to the current networking policy adopted by the Brazilian Air Force.

Summary

This chapter highlights the difficulty of linking distant BAF's points of presence due to the vast brazilian territory and the absence of computer communications capability at these remote points. The chapter also lists the objectives of the research, which are: (1) the determination of how BAF can use the Internet to establish an unclassified data communication network; (2) the estimation of costs of implementing and operating a VPN to integrate BAF's Material System units, and the comparison of these costs with the costs of using the current X.25-based alternative; and (3) the comparison of a VPN-based alternative and X.25-based alternative regarding security.

The research design is divided in four parts. The first part is the Review of Networking Security, which addresses basic security requirements for networks, the understanding of technical specifications of the TCP/IP, and the relation of the latter with threats and risks. Next, this review

exploits viable solutions such as cryptography, firewalls and packet filtering. The second part is the review of a Networking Cost Model, which studies the cost factors (cost drivers) involved in implementing and supporting a VPN-based alternative as well as a dedicated line-based alternative. The third part is the analysis of the Brazilian Public Network Infrastructure, which addresses the speed, reliability, security and cost of access of the brazilian backbone. The final part is the analysis of the BAF's Data Communication and Security Requirements, which identifies points of presence in order to come up with a feasible network topology and estimate the network load demanded.

Finally, the scope and limitations of the research are discussed. This includes issues regarding the availability of commercial hardware and software for network implementations, the currency used in the research, and the compatibility with the future implementation of the protocol Ipv6 (IP-Next Generation).

IV. Data Description and Results

Chapter Overview

This chapter presents the results and analysis of the procedures outlined in the previous chapter. It includes the evaluation of how the BAF's points of presence can be covered by X.25 dedicated lines (X.25 WAN). Based on this evaluation, the chapter proposes a network topology and calculates the associated costs. To provide a more precise analysis, a breakdown structure that divides costs into five categories is adopted and costs are then evaluated on a one-time setup basis as well as on a recurring monthly basis.

Regarding the implementation of BAF's VPN, the chapter analyzes two alternative VPN setups (LAN-to-LAN VPNs and Client-to-LAN VPNs), discusses techniques of deploying tunneled data, and evaluates commercial firewalls. Once these initial discussions are settled, the chapter proposes a network topology and calculates its associated costs. A similar cost breakdown structure used in the X.25-WAN alternative is adopted.

Finally, the chapter presents a comparison of costs between the alternatives, performs an analysis of payback time and discusses security issues.

Solutions for a BAF X.25 Dedicated Network

Chapter II presented the Brazilian Internet infrastructure as in March 1998. In order to connect all Points of Presence involved in the Materiel System (SISMA), as described in Chapter II, the Internet network topology was used to estimate the position of the links in a hypothetical X.25 Brazilian Air Force WAN. Links presented in Figure 2.10 were used to create the X.25 backbone, as shown in Figure 4.1:

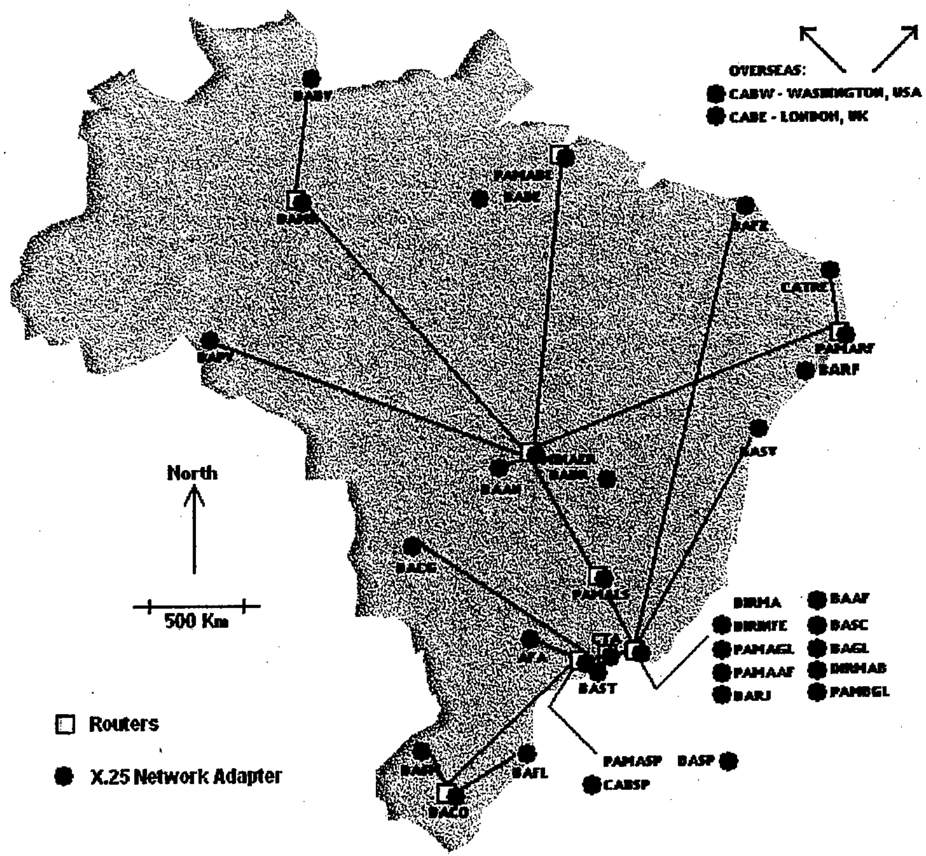


Figure 4.1 - Proposed Brazilian Air Force X.25 WAN

The network was built minimizing the distance between links, and using available links of the Brazilian Telecommunications infrastructure (RENPAC). A star bus topology is proposed, whose central links are implemented at Brasilia-DF, Rio de Janeiro-RJ, and São Paulo-SP, where probably the most intense network traffics are located. Sub-networks derive from these points, taking advantage of available X.25 links provided by RENPAC. A central router located at DIRINFE capable of handling heavy network traffic and routers at each branch are implemented in the proposed model. Additionally, the central router will handle international traffic (CABW and CABE).

Branching routers should be able to handle the local traffic, in locations where more than one unit are present, as well as traffic coming from remote locations branching from this location. An example is the router at PAMARF: this router should be able to handle traffic from the local sites (PAMARF itself and BARF) and from one remote branch (CATRE).

The following sites were selected to have branching routers:

- BAMN - handles local traffic and traffic coming from BABV;
- PAMABE - handles local traffic (PAMABE and BABE);

- PAMARF - handles local traffic (PAMARF and BARF) and traffic from CATRE;
- MINAER - handles local traffic (COMGAR, COMGAP, BABR, and BAAN) and traffic from remote sites and other branching routers (BAPV, BAMN, PAMABE, and PAMARF);
- PAMALS - handles local traffic (PAMALS) and bypasses to MINAER router;
- PAMASP - handles local traffic (PAMASP, BASP, CABSP, and BACG), remote sites (AFA and BAST), and BACO router;
- BACO - handles local traffic (BACO) and remote sites (BASM and BAFL);
- CTA - handles local traffic (CTA) and bypasses to PAMASP router; and
- DIRINFE central router - handles local traffic (DIRINFE, DIRMA, PAMAGL, PAMAAF, DARJ, BAAF, BASC, BAGL, DIRMAB, and PAMBGL), domestic remote sites (BASV and BAFZ), international remote sites (CABW and CABE), and branching routers PAMALS and CTA.

Cost Analysis of the X.25 Solution

1.0 - Network Access Costs

According to the Brazilian telecommunications company, the cost of using a X.25 dedicated line is composed of the following factors [56]: Carrier Costs = RENPAC 3025 costs

Dedicated Access costs + Port 3025 costs + Monthly utilized traffic costs (Domestic and International).

In order to compute Dedicated Access Costs, sites should be classified (referred to as "degrees") according to the geodesic distance between links. The classification of each site can be found in Appendix B, and the costs of each degree can be found in Appendix F. Table 4.1 summarizes the monthly dedicated access costs for the X.25 model proposed. There is an initial rate of $382.48 for each individual link of 9,600 bps. In addition to this initial charge, there is a fee that is proportional to the degree classification of each site. As a result, larger links are expected to be more expensive than shorter links.

Table 4.1 - Costs of X.25 Dedicated Access

RENPAC 3025 - X.25 - Monthly Dedicated Access Costs				
Degree	**Geodesic Distance**	**Number of Links**	**Monthly Access Cost**	**Total Monthly Access Cost**
1	Up to 50 KM	19	$ 382.48	$ 7,267.12
2	50 - 100 KM	0	$ 597.36	$ 0
3	100 - 200 KM	1	$ 657.55	$ 657.55
4	200 - 300 KM	3	$ 698.01	$ 2,094.03
5	300 - 500 KM	3	$ 758.54	$ 2,275.62
6	500 - 700 KM	1	$ 773.23	$ 773.23
7	700 - 1,000 KM	2	$ 783.01	$ 1,566.02
8	More than 1,000 KM	7	$ 802.75	$ 5,619.25
Total		**36**		**$ 20,252.82**

Source: Embratel - Brazilian Telecommunications [56]

Each X.25 port is charged $262.41/single port. For the 36 sites involved in the model, the total amount is represented on Table 4.2.

Table 4.2 - Costs of X.25 Ports

Ports Monthly Access Costs	
Number of Ports	36
Cost per Port	$ 262.41
Total	**$ 9,446.76**

Source: Embratel - Brazilian Telecommunications [56]

One aspect of the X.25 network cost model, is the additional charge for network traffic. The traffic cost is computed according to the number of segments of 64 octets (64 bytes) that is transmitted over the link. Firstly, the total number of segments was estimated according to the connection speed of 9,600 bps, and to the number of network links presented in the network. The total number of segments passing through the entire network can be computed as follows:

Number of bytes per second (maximum @ 9,600 bps) = 9,600 bps ÷ 8 bits/byte = 1,200 bytes/second

Total number of bytes per second = number of links × number of bytes per second = 34 links × 1,200 bytes/second = 40,800 bytes/second

Number of segments per second = total number of bytes per second ÷ 64 bytes/segment = 637.5 segments/second

Number of segments in one day = 637.5 segments/second x 3,600 seconds/hour x 8 hours/day (depot operational time)= 18,360,000 segments/day

Number of segments/month = 18,360,000 segments/day x 20 days (depot operational time) = 367,200,000 segments/month

Therefore, the traffic of the network was computed as 367,200,000 segments/month. However, an average of 50% of utilization rate was assumed, which results in 183,600,000 segments/month.

The cost of each segment was computed as the weighted average of the domestic traffic rate and the number of sites in each "degrees" as presented in Appendix F. The result was the value of $0.000781/segment based on the weighted average of the prices for each category (geodesic distances) and the number of units in each category. This yields a total amount of $143,391.60 for Domestic Monthly Traffic Costs. However, the Carrier (EMBRATEL) has discount rates based on the total number of segments transmitted in the network. The number of segments carried in the model corresponds to 45% of discount over the total amount of domestic traffic costs, as shown in the Table 4.3.

Table 4.3 - Domestic X.25 Traffic Costs

Domestic Monthly Traffic Costs	
Connection Speed	9,600 BPS
Number of bytes/second	1,200 bytes/sec
Number of Links	34 (excluded overseas)
Total WAN Throughput/second	40,800 bytes/sec
Total Segments/month (@ 50% utilization rate)	183,600,000 segments/month
Cost per segment transmitted	$ 0.000781/segment
Total Cost before discount	$ 143,391.60
Discount (segments)	45 %
Total Cost	**$ 78,865.38**

Source: Embratel - Brazilian Telecommunications [56]

International Traffic costs are computed in the same way as in the domestic case, but the cost of each segment carried is defined by the Carrier Company as $0.01316/segment.

Table 4.4 - International X.25 Traffic Costs

International Monthly Traffic Costs	
Connection Speed	9,600 bps
Number of bytes/second	1,200 bytes/sec
Number of Links	2
Total WAN Throughput/second	2,400 bytes/sec
Total Segments/month (@ 50% utilization rate)	1,024,000 segments/month
Cost per segment transmitted	$ 0.01316/segment
Total Cost before discount	$ 13,475.84
Discount (segments)	45 %
Total Cost	**$ 7,411.71**

Source: Embratel - Brazilian Telecommunications [56]

Consequently, the total cost of networking would be $115,976.67, as shown in Table 4.5.

Table 4.5 - Total X.25 Carrier Costs

Total Carrier Costs	
Dedicated Access Costs	$ 20,252.82
Port Costs	$ 9,446.76
Domestic Traffic Costs	$ 78,865.38
International Traffic Costs	$ 7,411.71
Total Monthly Carrier Costs	**$ 115,976.67**

2.0 - Hardware Costs

Hardware costs are represented primarily by costs involved in the procurement of equipment necessary to operate the network in the X.25 protocol environment. That equipment consists basically of routers, hubs, and X.25 Network Adapter Cards.

Segmented links should be joined to the main network through the use of remote bridges or routers, as in the case of the segment BASM-BACO-BAFL in the south portion of the proposed X.25 WAN. The central point connected to the main segment is the BACO Local Area Network, and the remote segments are the BASM and BAFL Local Area Networks. In that case, a transparent Wide Area Network can be implemented in a segmented remote access environment. Equipment capable of handling up to 10 branches and operate at throughput of 9,600 bps, such as Cisco's 2505 Router and 3Com's SuperStack II 221 bridges, can be used in this case [57, 58].

The central server point (assumed to be BAF's DIRMA) should be connected to the remote links through a router capable of dealing with a greater number of connections, when compared with remote routers. At this point, the central router should be able to handle the connection requisitions of all remote and local clients. Therefore, more robust equipment should be used in this site. Equipment such as Cisco's 2507 Router or 3Com's SuperStack II 228 Router can be used in the central network point [57, 58].

In addition to the equipment necessary to "build" the essential network backbone to connect all sites, each individual site might have a Local Area Network. However, this study only considers the final point of connection to the main backbone at each site. Consequently, the minimum necessary equipment is a X.25 Network Adapter and a synchronous modem. In this study, an integrated X.25 adapter and modem such as Digi's DataFire SYNC/570I-56 synchronous X.25 adapter card [59] is used. The estimated hardware requirements and costs are illustrated in Table 4.6.

Table 4.6 - X.25 Hardware Costs

Hardware Costs Network Equipment	Quantity	Unit Price	Total Price
CISCO 2507 Router	1	$ 5,050.00	$ 5,050.00
CISCO 2505 Router	9	$ 4,000.00	$ 36,000.00
X.25 Network Adapter	36	$ 1,500.00	$ 54,000.00
Total			**$ 95,050.00**

3.0 - Software Costs

Software costs in the X.25 model are assumed to be irrelevant, given that this research proposed to provide point-to-point communications capability. Communications software to handle X.25 protocol is assumed to be part of the operating system elected to be operated, or additional software to operate in this environment would be provided by the network adapter manufacturer.

4.0 - Maintenance Costs

This study assumes a cost per maintenance action (MA) of $1,000/MA for routers and $500/MA for network adapters in a project life cycle of 5 years. Given the MTBF provided by the equipment manufacturers of 50,000 hours, we were able to calculate the number of maintenance actions in 5 years (TBF assumed exponentially distribution)is calculated as follows: MTBF = 50,000 hours; Life-cycle = 5 years × 365 days × 24 hours/day = 43,800 hours. Therefore, this study uses

approximately one maintenance action per piece of equipment during the life-cycle.

This leads to maintenance costs of 39 × \$500 + 10 × \$1,000 = \$29,500/project life cycle, or \$5,900/year (approximately \$500/month).

5.0 - Training and Support Costs

Although the Brazilian Air Force already has personnel with knowledge in implementing X.25 networks, additional costs should be taken into account in order to support the greater number of sites and links. We assumed that 3 persons with technical skills in networking (level of Sargent) would be the minimum necessary to accomplish support tasks. In order to train these personnel, we estimate that the costs would be \$3,000/person given the price of networking courses in Brazil. In that way, training costs would be \$9,000/life-cycle.

A second or third-Sargent costs for the Brazilian Air Force approximately \$20,000 annually. This value suggests that in order to maintain and support the X.25 network, the costs would amount to \$60,000/year (approximately \$5,000/month).

6.0 - Summary of X.25 Model Costs

Table 4.7 represents the summary of costs referent to the implementation of the X.25/leased lines solution.

Table 4.7- Summary of X.25 Costs

Category	One-time setup	Monthly
Network Access Costs	N/A	$ 115,976.67
Hardware Costs	$ 95,050.00	N/A
Software Costs	N/A	N/A
Maintenance Costs	N/A	$ 500
Training and Support Costs	$ 9,000	$ 5,000
Total	**$ 104,050**	**$ 121,476**

Solutions for Implementing a Virtual Private Network

Pfaffenberger [27] proposed six models of extranets (or Virtual Private Networks) topology. The models are described as: a weakly authenticated Web Server; a strongly authenticated Web Server; strongly authenticated access to internal resources with access control; strongly authenticated access using object-oriented middleware; LAN-to-LAN Virtual Private Network; and finally Dialup Virtual Private Network.

Because the present study deals with the creation of a extranet interconnecting resources in all sites instead of using only Web-based solutions, it is proposed that the Brazilian Air Force model be a mix of the LAN-to-LAN VPN and the Dialup VPN models. This model would use tunneling

technology to provide confidentiality and integrity of messages and to integrate all BAF's LANs into a seamless disperse local area network.

LAN-to-LAN Virtual Private Networks links two or more LANs through the insecure public Internet. The suggested configuration [27] is composed of a tunnel server and a firewall in each link of the individual LANs to the Internet. Babcock [60] suggested that for a configuration with improved security, the firewall should be placed in front of the VPN (tunneling server). A tunneled channel is established between two LANs using strong encryption, authentication, and access control in the Figure 4.2.

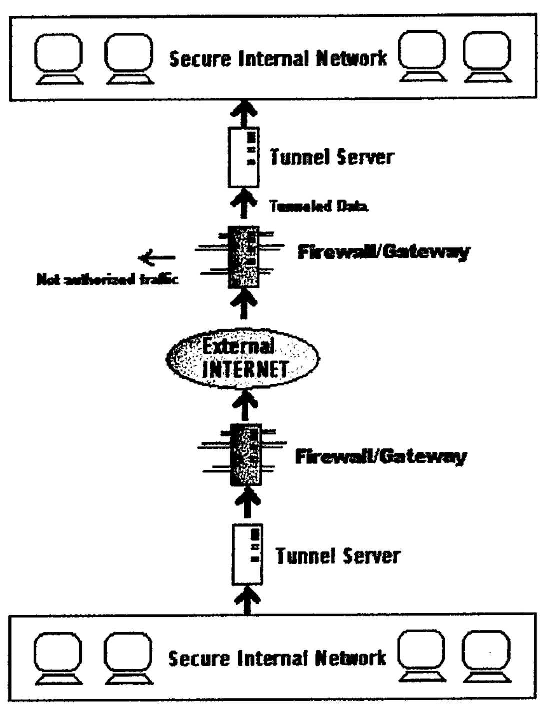


Figure 4.2 - LAN-to-LAN suggested VPN setup [27]

Dialup Virtual Private Networks connections - sometimes called client-to-LAN VPNs - between a client and a "remote" Local Area Network are established using techniques similar to the LAN-to-LAN VPN. However, instead of using a tunnel server, the remote client itself or the Internet Service Provider (where available with this feature) is in charge of tunneling the data through the Internet. However, there are some drawbacks in this configuration, for instance, degradation of the bandwidth and extra processing resources in the client system.

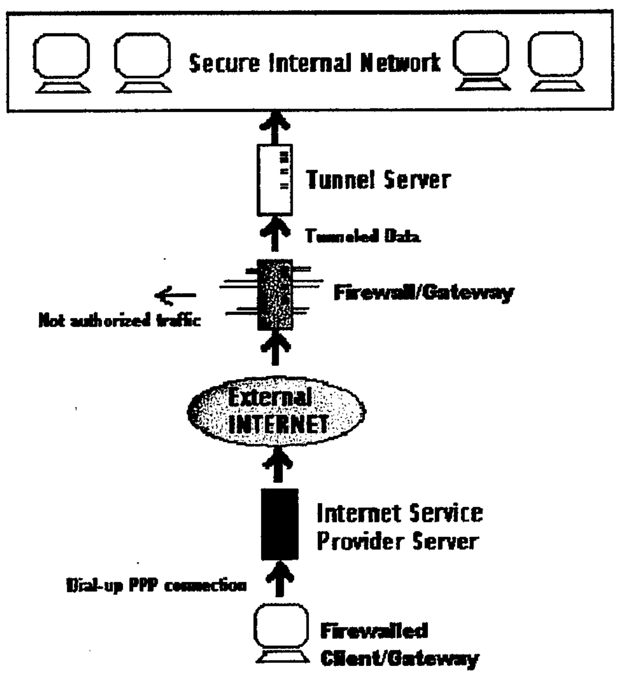


Figure 4.3 - Client-to-LAN suggested VPN setup [27]

The Internet Engineering Task Force (in reality, the IPSec working group) is currently working on a deployment of a secure channel through the Internet (or a VPN):

> IETF is developing a standardized key management mechanism that enables safe and secure negotiation, distribution and storage of encryption and authentication keys. A standardized packet structure and key management mechanism will facilitate fully interoperable third party VPN solutions. [50]

This mechanism is the so called IPv6 or IPSec.

In the mean time, there are four major techniques of deploying tunneled data: Point-to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP), and Socksv5. The white paper "Virtual Private Network Security Components" from CheckPoint Software [50], one of the VPN software vendors, presented the following call out scheme in order to explain the deployment techniques:

> Point-to-Point Tunneling Protocol (PPTP) - An extension of Point-to-Point Protocol (PPP) that encapsulates IP, IPX, or NetBEUI inside IP packets, this protocol is used primarily by ISP equipment providers because it accommodates end to end and server to server tunneling. Largely a proprietary protocol, only recently was a proprietary encryption mechanism added, which is still considered optional.
>
> Layer 2 Forwarding (L2F) - A forwarding protocol used to "tunnel" higher level protocols into a link layer protocol (i.e., HDLC, asynchronous HDLC, or SLIP frames). Although this facilitates remote dial-in connectivity,

the information in an L2F traffic stream in not encrypted.

Layer 2 Tunneling Protocol (L2TP) - A protocol that tunnels PPP traffic over a variety of networks (e.g., IP, SONET, ATM) and is used to provide multi-protocol dial-in services for Internet Service Provider's (ISP) Point of Presence (POP). Like L2F, L2TP does not define any sort of data privacy mechanism (encryption). Further, a draft exists which proposes the use of the IPSec protocol suite to provide data privacy of L2TP traffic over IP networks.

Socksv5 - An IETF protocol defining how client-server TCP and UDP applications are handled via a proxy server. VPN solutions based on Socksv5 technique is essentially a proxy based VPN implementation, which is no different than any other proprietary proxy-based VPN solution. The fact that Socksv5 is an IETF protocol does not provide any interoperability benefit one would expect from a standard-based VPN implementation, such as one based on IPSec.

Broderick et al. [61], Stern [4], Bruno [62], Lipschutz [36], and Newmann et al. [35] tested several commercial Firewalls and Virtual Private Network solutions based on several authentication and encryption schemes, and deployment techniques. The results of benchmarks and simulated attacks suggested that solutions based on the IPSec protocol are more robust and secure.

Stern [4] analyzed ten Virtual Private Network software-based solutions: AltaVista Tunnel 97 (Digital Equipment Corporation), Aventail VPN 2.5 (Aventail), Firewall-1 3.0a (CheckPoint Software Technologies), F-Secure Virtual Private Network 1.1 (Data Fellows), FTP Software

Secure Client 3.0, Microsoft Routing and Remote Access Service (Microsoft Corporation), Raptor Eagle NT 4.0 (Raptor Systems), Secure Computing BorderWare Firewall Server 4.1 (Secure Computing), SunScreen SKIP 1.1 (Sun Microsystems), and TIS Gauntlet 4.0 (Trusted Information Systems). According to the article, the top performance and features selected solution is the Aventail VPN 2.5.

Given these results, this study selected as possible options Aventail VPN 2.5, CheckPoint FireWall-1 3.0a, and Raptor Eagle NT 4.0. These solutions include support for LAN-to-LAN and client-to-LAN connections, IPSec compliant (RFC 1825 [63]), RC4 and RSA encryption schemes, and support for Windows (as client for Win 9X and NT and server for Win NT) and Unix environments. Appendix E presents the technical characteristics of these solutions.

Newmann et al. [35] made a thoroughly analysis of 19 firewall and VPN solutions, and included assessments of remote management capabilities and access control capabilities, multiple servers access control, denial-of-service attacks (SYN flooding, Ping of Death, Log full, and Disk full), and an extensive study of logging capabilities. According to the authors, the awarded solutions were CheckPoint's Firewall-1, Cyberguard Firewall, Seattle

Software Labs' Watchguard Security System 200, and Sun's SunScreen EFS.

Lipschutz [36] also analyzed five Windows NT-based Firewall solutions: AltaVista Firewall 97 (Digital Equipment Inc.), CheckPoint Firewall-1 (CheckPoint Software Technologies), Guardian (LanOptics Inc.), NetRoad Firewall (Ukiah Software Inc.), and Raptor Eagle NT (Raptor Systems Inc.). Once again, CheckPoint's Firewall-1 was selected by the author as the awarded firewall solution.

The objective of this research, as stated in Chapter I, is to develop a Virtual Private Network independent of hardware and operational system platform, with the best tradeoff between cost and security. The proposed model is based on CheckPoint's Firewall-1 solution, given that this solution has presented good indices of performance and cost according to several benchmarks.

Additionally, the recommendations of Cheswick [64] are adopted in this study. He suggested that an Internet gateway should be allocated to each network node to the Internet. The Internet gateway is described as an "application-level gateway that passes mail and many of the common Internet services between our [the] internal machines and the Internet." At first, it can be misunderstood as the description of another firewall device, but in reality it

adds additional protection by performing some inbound and outbound services such as filtering, logging, and periodically check of the system and protected network.

Proposed TCP/IP Network Topology

Given that all Points of Presence are physically located in sites currently served with Internet Service Providers, this study established the approximate network traffic for each site, and classified sites according to the following arbitrary scale: Class A sites - Command sites; Class B sites - Depots and Major Bases; and Class C sites - otherwise. This classification was based on the amount of logistics support provided by the PAMASP depot in the year of 1997.

Class A sites would be connected to the TCP/IP network through dual-ISDN connections (128 Kbps), Class B sites would be connected through single-ISDN devices (64 Kbps), and Class C sites would be connected through regular dial-up modem connections. In the last case, the throughput is determined by the limit imposed by the ISP-side dial-up devices. It is recommended that all Class C sites use 56 KBPS V.90 devices. The study has shown that ISP connection limits vary from 14,400 bps in certain regions (North and Northeast) close to 56,600 bps in others (mainly in the

Southeast region). Appendix B presents the suggested classification of each unit involved in the Brazilian Air Force Materiel System (SISMA).

This study proposes the creation of a strategic virtual Brazilian Defense backbone linking the Brazilian Air Force's major depots and commands. This virtual backbone would be composed of T1 links directly to the Brazilian Carrier Company (Embratel); however, given the assumed traffic of data, the use of T1 connections could be over dimensioned.

The proposed configuration consists of off-site and on-site connections from the headquarters. Remote users may be based anywhere in the Brazilian territory, as well as overseas locations, as indicated in Appendix B. It is assumed that the TCP/IP network protocol suite is used in all units. This seems reasonable, given that all current operating systems and platforms have native support for these protocols. However, little or no disruption of daily activities can be accomplished with the addition of a protocol-converter gateway (such as NetBEUI-TCP/IP, or IPX-TCP/IP) just before the VPN server.

The applications that would be used in this configuration include mailing, print and file sharing, web browsing, FTP, remote control capabilities, and distributed components. Additionally, this study assumes that

eventually distributed database systems would use some allocated TCP port and configuration to transmit data. As in the current model, all database servers would be physically located at DIRINFE (Rio de Janeiro), and Web servers and Mail servers would be located at DIRMA (Rio de Janeiro). In order to compute the bandwidth required at these locations, we assumed the percentage of concurrent usage as 20%, i.e., 20% of the total number of users of the network would be using competing resources at the same time. We also assumed that 95% of the time connections would be at full modem/network card capacity. The bandwidth requirement for Class A sites can be computed as [65]:

Class A External Bandwidth = Total Number of Users Class B x % Concurrent Connections x Network Utilization Factor (Internet) x Line Speed of Class B connections + Total Number of Users Class C x % Concurrent Connections x Network Utilization Factor x Line Speed of Class C connections = 8 x 10% x 95% x 56 KBPS + 22 x 10% x 95% + 9.6 KBPS = 105.1 KBPS nominal

This suggests that Class A locations are each eligible for one "1/4" T-1 connection (386 KBPS) or "dual" ISDN connections (128 KBPS) to the backbone. In that case, a dual-ISDN seems more reasonable in terms of cost. For the computation of Class B requirements, this study uses a single ISDN connections with 64 KBPS of throughput.

In the proposed model, using CheckPoint's Firewall-1 VPN solution, Class A and B sites would be connected to the Internet backbone through a firewall (in that case, a Firewall-1 equipment) and an additional gateway in order to provide improved authentication mechanisms and protection against attacks (typically denial-of-service attacks). The configuration is shown in the Figure 4.4:

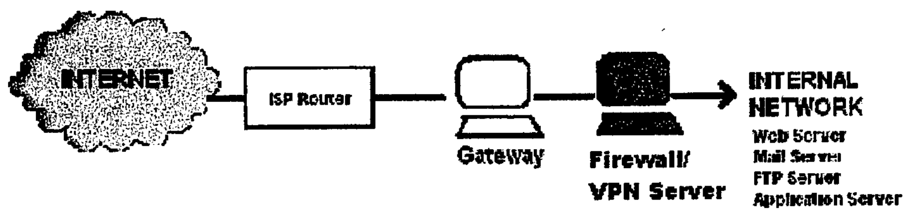


Figure 4.4 - Classes A and B VPN setup

Class C sites would be connected to the Internet through a regular dial-up modem connection. In that case, the firewall would act also as a proxy server based on CheckPoint's Firewall-1 solution; and the same level of security can be accomplished through the use of a front-end gateway.

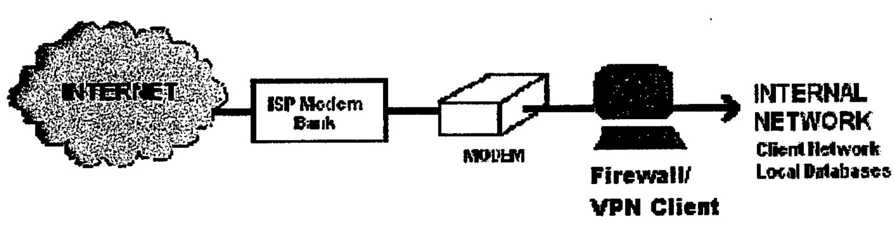


Figure 4.5 - Class C VPN setup

Cost Analysis of the VPN Solution

1.0 Networking, Hardware and Software Costs

For each Class C site, the following equipment would be used: one 56 KBPS V.90 modem, one Pentium II machine equipped with network cards configured as firewall, one gateway machine, and one hub for connection with the internal network. Client machines are not taken into account in the model comparison, because the cost of these machines are sunk costs. Regarding software, one license of an operating system such as MS Windows NT 4.0 Server, Linux or FreeBSD must be used. These last two options are free of charge, however little or no support is guaranteed. One license of the "client" firewall should be bought in order to build the firewalled gateway between the internal network and the public Internet. Regarding connection fees, access to the Internet would be provided by local Internet Service Provider at each individual site. In general, Brazilian ISPs charge a fixed monthly fee for 20 hours/month, although they are moving toward unlimited access fees.

In addition to ISPs fees, local phone charges should be taken into account. In contrast to North American phone companies, Brazilian companies charge by "pulses" of 3 minutes of connection. Each pulse is charged by

$0.05/pulse; therefore, supposing 40 hours of weekly access, the amount charged by local companies is about $200.00/month for each site. The summary of equipment and software cost for each Class C site can be found in the Table 4.8:

Table 4.8 - Hardware, Software, and Internet Access Costs for Class C sites

Category	One-time Cost	Charge/Month
Hardware		
Modem 56 KBPS V.90 compatible	$ 150	-
Pentium II machine (firewall)	$ 2,000	-
Pentium machine (gateway)	$ 1,000	
10/100 Ethernet Card	$ 50	-
10/100 Hub (10 ports)	$ 100	-
Software		
Firewall Software	$ 3,000	-
Gateway Software	N/A	-
Internet Access		
ISP Monthly Access	$ 40	$ 40
Telephony Company Access	-	$ 200
Total Per Site	**$ 6,340**	**$ 240**

Class B sites would also be connected to the Internet through an ISP router, but at a higher speed by using ISDN devices. Therefore, instead of a regular modem, it is necessary to use a special ISDN modem.

ISDN devices are still not very common in Brazil; however, in the principal cities (where Class B sites are primarily located), there are a considerably number of ISPs with this capability. The Brazilian telecommunication legislation imposes a fee of $450.00/month for ISDN access of 64 KBPS over digital lines installed in the main cities.

The costs associated with each Class B sites are represented in Table 4.9.

Table 4.9 - Hardware, Software, and Internet Access Costs for Class B sites

Category	One-time Cost	Charge/Month
Hardware		
ISDN 56 KBPS Modem	$ 250	-
Pentium II machine (firewall)	$ 2,000	-
Pentium machine (gateway)	$ 1,000	
10/100 Ethernet Card (3 EA)	$ 150	-
10/100 Hub (10 ports)	$ 100	-
Software		
Firewall Software	$ 3,000	-
Gateway Software	N/A	N/A
Internet Access		
ISP Monthly Access	$ 700	$ 1,000
Telephony Company Access	-	$ 450
Total Per Site	**$ 7,200**	**$ 1,450**

Class A sites would also be connected to the Internet through an ISP router, but at higher speed by using dual-ISDN devices connected at 128 KBPS. The Brazilian telecommunication legislation imposes the fee of $650.00/month for ISDN access of 128 KBPS.

In order to assure additional protection against attacks and non-authorized access to internal information, a gateway configured as a packet-filtering device will be installed just before the connection to the public Internet backbone. A standard firewall configured as a tunnel server is the next link after remote connections are authenticated.

The following table illustrates equipment and connection costs (set-up and monthly fees) involved in each Class A site.

Table 4.10 - Hardware, Software, and Internet Access Costs for Class A sites

Category	One-time Cost	Charge/Month
Hardware		
ISDN 128 KBPS Modem	$ 400	-
Pentium II machine (firewall)	$ 2,000	-
Pentium machine (gateway)	$ 1,000	
10/100 Ethernet Card (3 EA)	$ 150	-
10/100 Hub (10 ports)	$ 100	-
Software		
Firewall Software	$ 3,000	-
Gateway Software	N/A	N/A
Internet Access		
ISP Monthly Access	$ 700	$ 2,200
Telephony Company Access	-	$ 650
Total Per Site	**$ 7,350**	**$ 2,850**

Table 4.11 represents the aggregated costs of network access, hardware, and software for the Virtual Private Networking solution.

Table 4.11 - Aggregated One-time and Monthly Hardware, Software, and Internet Access Costs for the VPN Solution

CLASS	Number of sites in the Class	One-time VPN Cost	Total One-time VPN Cost	VPN monthly Cost	Total VPN monthly Cost
CLASS A	3	$ 7,350	$ 21,750	$ 2,850	$ 8,550
CLASS B	11	$ 7,200	$ 78,100	$ 1,450	$ 15,950
CLASS C	22	$ 6,340	$ 139,480	$ 240	$ 5,280
Total	**37**		**$ 240,730**		**$ 29,780**

2.0 - Maintenance Costs

In a VPN environment, little or no maintenance is required for equipment. The suggested approach, according to Pfaffenberger and other authors is to consider hardware as consumable parts [27]. In that way, if a modem malfunctions, the solution is to replace the equipment with a new one. Assuming that 30% of the equipment will fail in the life-cycle period, the hardware maintenance costs are estimated as $120,650 × 30% = $36,195 in the five-year period (about a $600 per month).

However, software maintenance costs could be far greater than hardware maintenance costs. Software maintenance costs involve configuration management, bug tracking, updates and patches installation, and version control. Those costs will be included as supporting costs.

3.0 - Training and Support Costs

Currently, the Brazilian Air Force does not have sufficient personnel in the area of network security and Information Warfare. In order to implement direct connections to the Internet, and in this way potentially exposing logistics information to all sort of unauthorized access, the Brazilian Air Force should be able to deal with

this problem not only through the use of leading technology such as strong encryption and firewalls, but by building a team of professionals involved full time on tracking bugs and holes in operational systems and software and on studying new exploits and hacking tools. This team should have the tools and knowledge to do risk-assessments, to perform controlled attacks, to be engaged on detecting and acting against attacks and intrusions, and to be mobilized in a planned fashion in the case of an eventual successful attack/intrusion against one site or the entire network.

Building this infrastructure responsible to perform important tasks in the Information Warfare (IW) context is not just a technical matter, but also a political issue.

The costs to implement an entire IW infrastructure will not be addressed, but just the costs associated with the implementation of a core of specialists in network security to deal with the Virtual Private Network security issues. It is estimated that three to five highly qualified professionals with IT backgrounds would be needed to work in the BAF's Computer Emergency Response Team nucleus. In order to train four persons in advanced networking and security, and additionally each one in a specific operating system environment (Sun Solaris, Windows NT, Linux, etc), it is estimated that the BAF would spend the minimum of $15,000

for each individual. This cost is undoubtedly higher than training in networking problem solving as required in the X.25 model, and reflects the high level of knowledge and technical expertise required to be prepared to work on this area.

Several organizations [1, 33, 62] have tried to quantify the costs in terms of dollars of unauthorized access and attacks to their networks. The cost is estimated to be around $3,000 for minor successful abuses, more than $100,000 for service disrupting and root control attacks, and more than $1.5 million for theft of proprietary information. In an Information Warfare context, the cost of successful attacks should be more difficult to compute and probably be much more costly than in the commercial sector. Disruption of information systems (assuming that the BAF would rely solely on computers) for one day could incur logistics and administrative costs of more than $100,000/day. Airplanes could be grounded; supply requisitions could be delayed; personnel paychecks could be not processed on time; meaning all kinds of problems and indirect costs related to the same problem. The US DoD reported that an incident involving disruption of an entire research system by hackers in the Rome Laboratory in 1994 alone cost over $500,000.

The incidence of attempts to attack military computers is much higher than in the commercial sector. Perhaps the reasons for this phenomenon is that the commercial sector still feels that announcing attacks could hurt the organizational image with the consumers [1, 5]. The fact is that in the United States, the Defense Information Systems Agency (DISA) reported that in 1995 the agency had experienced more than 250,000 attacks, of which 65% of attacks were successful [1]. These numbers can represent a serious threat to the National Security. Meanwhile, in the United States, the Department of Defense is taking actions to address this problem and react immediately to attacks. The solution to minimize intrusions and attacks is to implement an aggressive, proactive detection, and reaction program [1].

In order to make a comparison and to estimate a "probable" number of attacks against the BAF network, this study collected information about the size of the United Stated Defense Network. According to the GAO, the US Department of Defense in March 1996 accounted with 2.1 million computers, 10,000 LAN's, 100 WAN's, 200 command centers, and 16 central computer processing facilities. These numbers are far greater than the number of computers and networks installed in the Brazilian Air Force. With the implementation of the VPN, the BAF would account with less

than 1% of the total number of computers and networks presented in the US Defense Network. However, one cannot assert that the number of attacks experienced by an organization is directly proportional to the number of computers and networks, but perhaps is proportional to the number of sites with poor protection against attacks. Either cases, no data was available to extract such information.

Therefore, assessing the expected number of attacks is even more difficult if knowledge that a military incipient network was being built attracts a great number of "testers." Even a rough estimation cannot be made at this level of information. Therefore, the costs related to response evaluation will be ignored in this study, while costs related to prevention (proactive technical protection, monitoring, auditing) will be overestimated.

In order to build a complete emergency response capability, additional tools such as auditing trail tools, port and service scanners, remote control and administering tools and special equipment should be procured. Estimations amount to the value of $100,000 [66] in order to procure those tools and train the personnel involved in this task. Therefore, the cost of support in the case of a VPN implementation is summarized in Table 4.12:

Table 4.12 - Brazilian Air Force CERT Implantation Costs

Category	Costs	Base
BAF CERT Training	$ 60,000	One-time
BAF CERT Personnel Salary	$ 80,000	Yearly
Tools and Equipment	$ 100,000	One-time
Tools and Equipment Maintenance and Updates	$ 10,000	Yearly (assumed as 10% per year of the total amount)
Installation Overhead	$ 2,000	Monthly

4.0 - Summary of VPN Model Costs

Table 4.13 represents the summary of costs referent to the implementation of the TCP/IP-Internet solution.

Table 4.13 - Summary of VPN Costs

Category	**One-time setup**	**Monthly**
Network Access Costs	$ 10,680	$ 29,780
Hardware Costs	$ 122,050	-
Software Costs	$ 108,000	-
Maintenance Costs	-	$ 600
Training and Support Costs	$ 160,000	$ 9,500
Total	**$ 400,730**	**$ 39,880**

Summary of Costs in the X.25 and VPN models

The following table summarizes one-time and monthly costs presented in both solutions in order to compare costs and establish the Payback period of the VPN model.

Table 4.14 - Summary of Costs of X.25 and VPN

	X.25 Model		VPN Model	
	one-time	**Monthly**	**one-time**	**Monthly**
Hardware	$ 95,050	-	$ 122,050	-
Software	-	-	$ 108,000	-
Network Access	-	$ 115,976	$ 10,680	$ 29,780
Maintenance	-	$ 490	-	$ 600
Training	$ 9,000	-	$ 60,000	-
Support	-	$ 5,000	$ 100,000	$ 9,500
TOTAL	**$ 104,050**	**$ 121,466**	**$ 400,730**	**$ 39,880**

As table 4.14 shows, the "start-up" costs of the VPN model are higher than the "startup" costs of a x-25 model, but the monthly costs of the VPN model are lower. Consequently, the payback period, i.e., the number of years or months in which the VPN solution pays for itself, can be computed using the cash-flow presented in Figure 4.6.

Assuming an inflation rate of 1% per month, we can compute the payback-period value *n* as:

$$296{,}180 = \sum_{i=1}^{n} \frac{81{,}586}{(1+0.01)^{i}}, \text{ and } n \cong 3.5 \text{ months}$$

Therefore, the payback period is approximately 4 months.

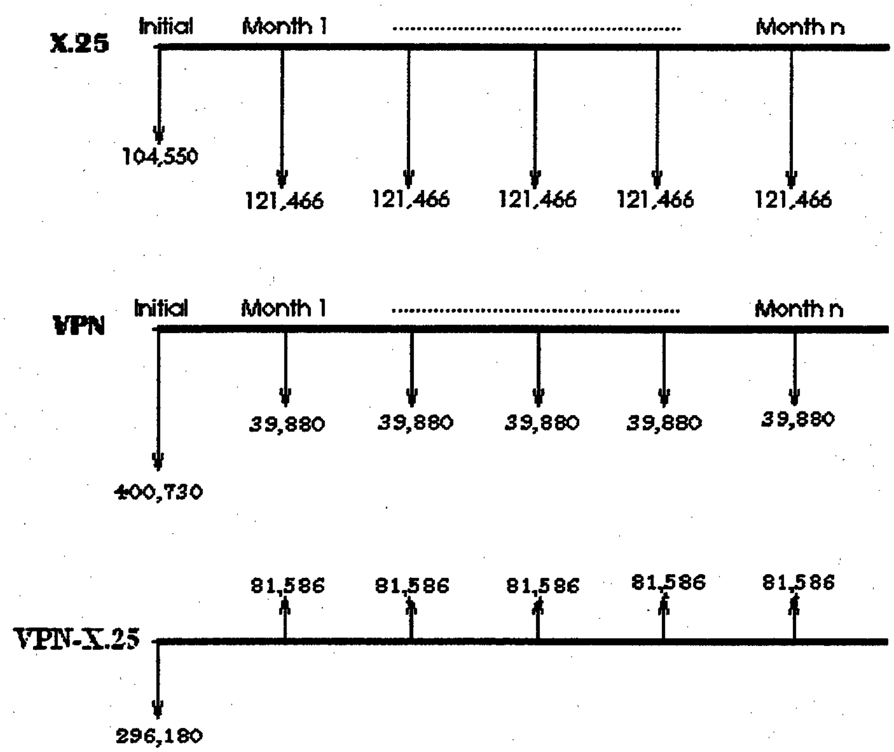


Figure 4.6 - Payback period computation

Security Analysis of X.25 and VPN models

Chapter II presented some concepts of networking and computer security. Those fundamental concepts are authentication, access control, integrity, confidentiality, non-repudiation, and guarantee of access for trusted users.

Additionally, the threats related to each of the individual layers of the OSI networking model were discussed.

All authors of the security field agree that before the implementation of a "secure" network with the last technological breakthroughs such as strong encryption, firewalls and VPN servers, a complete, detailed, and consistent security policy should be implemented. This affirmation leads to the conclusion that enforcement of the security policy on a daily basis is also important. Several authors recommended the adoption of a Computer Emergency Response Team in order to make the necessary security enforcement, risk assessment, and response to attacks and potential threats.

The X.25-leased lines and TCP/IP-Internet security models are evaluated by comparing the threats at each level of the OSI model. This study was based on a C2 level security system for the VPN model, and used the current model of leasing lines without any treatment of the packets for the X.25 model.

For the X.25 model, threats of each layer are shown in the Table 4.15. It is important to emphasize that it could be possible to implement a more tight security scheme for the X.25 network with the utilization of firewalls and packet filters for a packet switching network such as the

X.25 specification; however, as stated in the assumptions, this study is only considering the current level of protection of the Brazilian Air Force network model.

Table 4.15 - X.25 model network security threat levels

OSI Layer	Type of Attack	Extent of threat	Level of "hacking"	Solution
Physical	RF Eavesdropping Cable Eavesdropping Man-in-the-middle attack	Reading, Denial of Service	Physical access to cables on carrier. High Level of Information Warfare.	No Effective Solution with present model
Data Link	Man-in-the-middle attack	Reading, message alteration, integrity	Physical access to routers/cables on carrier. Medium Level of IW.	Physical protection of Routing points
Network	Message Replay Routing attack	Reading, message alteration	Access to routing tables on carrier. Medium Level of IW.	Physical protection of Routing points
Transport	Depends upon the higher level protocol used	Reading, DoS, message alteration	Access to any point of the packet-switching network. Medium Level of IW.	No Effective Solution with present model
Application	Depends upon the higher level protocol used, but guessed passwords are most likely.	Access control, DoS	Access to router, or physical access to cables and routing tables. Trojans, Social Engineering. Low Level of IW.	No Effective Solution with present model

For the VPN model, at a C2 level using the Internet and TCP/IP suite protocols, threats of each layer are shown in the Table 4.16.

Table 4.16 - TCP/IP-Internet network security threat levels

OSI Layer	Type of Attack	Extent of threat	Level of "hacking"	Solution
Physical	RF Eavesdropping Cable Eavesdropping Bombing of cables	Reading, Denial of Service	Physical access to cables on carrier or ISPs. High Level of Information Warfare.	Encryption, cables shielding, expansion of routing points
Data Link	Man-in-the-middle attack	Reading, message alteration	Physical access to routers/cables on carrier. Medium Level of IW.	Encryption and authentication
Network	Message Replay Message Delay Routing attack Spoofing, Sniffing, Trusted-access attack	Reading, message alteration, integrity	Access to any point of the Internet. Low Level of IW.	Access Control, filtering, IPSEC, authentication
Transport	Session Hijacking, IP spoofing	Reading, DoS, message alteration	Access to any point of the Internet. Low Level of IW.	Encryption, authentication, nonrepudiation
Application	Root control, guessed passwords, Trojan, Data and Software vulnerabilities	Access control, DoS, reading	Exploitation of holes and bugs, virii, trojans, access to the Internet, Social Engineering. Low Level of IW.	Access Control, Filtering, direct enforcement of security policy

Comparing the X.25 solution with the VPN solution, one can see that for a higher level of Information Warfare, both solutions have common threatening points. In reality, the VPN solution presents more threats at a lower level of IW than the X.25 solution. With VPN, much more attempts of attacks from the outside and "probing" are expected.

The security of the X.25 solution depends basically on the level of access control to the physical cable and routers on the carriers and telecommunication links [71]. It requires enormous interest by the attacker on eavesdropping messages and disruption of C3 systems to accomplish attacks at this level.

Even so, it is almost impossible to guarantee this level of protection without the use of the same tools such as encryption, authentication and access control as in the VPN model. Therefore, in order to achieve a higher degree of security in the X.25 model, the same type of equipment (firewalls, packet filters, gateway, etc.) is required.

The selected VPN solution Firewall-1 from CheckPoint Software is complaint with C2 level and more [67], and has security characteristics as shown in Appendix E. It operates with three levels of symmetric encryption: RSA, 3-DES (IPSec standards), and a proprietary algorithm called FWZ-1; and two public-key schemes: RC4 and DSS (Diffie-Hellman). For authentication and data integrity, this solution employs MD5 and SHA-1. According to the Firewall-1 developer, with these encryption and authentication methods, it "supports encryption speeds greater than 10 Mb/sec through a standard desktop workstation" [86]. This level of throughput is more than sufficient for the VPN model, and it

permits future expansions of the network without the need of new firewall equipment if the traffic reaches the equivalent of up to six full T1 lines.

Regarding Access Control, the VPN solution has the capabilities of network address translation and stealthing, i.e., it can hide its access point and make the device invisible from outside access. It can also permit the implementation of "honey-pots" for capturing remote connections with "not so good" intentions (prospectors). Additionally, the Firewall-1 has advanced auditing, logging, and alarming features.

The gateway installed between the insecure public network and the firewall server can provide additional security by creating a "militarized zone" by filtering and screening packets from unrecognized addresses and content. This additional protection can isolate the network segment by creating a trusting relationship between the gateway and the firewall server. Moreover, the gateway server has to be configured with the minimum number of services, and should be the first to be patched and its security enforced (operating system hardening). An extended logging capability should be implemented on the gateway, for additional tools for auditing and security assessment.

Risk assessments from the internal network and from the external branch should be made [69]. Software tools such as

SATAN (for Unix), Network Associate's CyberCop, and several network scanners can be used in order to make real intrusion attempts and assessment of security level.

Summary

After an evaluation of the Brazilian Internet Infrastructure, the solution for a BAF's X.25 dedicated network is found to be a star bus topology. Its central links are located at Brasilia-DF, Rio de Janeiro-RJ, and São Paulo-SP. To handle heavy local traffic and international traffic, a central router is located at DIRINFE, and in areas in which there is more than one unit, branching routers are installed. The costs of the BAF's X-25 WAN are divided into five categories: network access costs, hardware costs, software costs, maintenance costs, and training and support costs. Each one of these categories is analyzed on a monthly basis and on a one-time setup basis. The final costs of implementing a X.25 WAN include a one-time setup cost of $104,050 and a monthly cost of $121,476.

Regarding the implementation of a VPN solution, all BAF's points of presence are located in areas that provide Internet Service Providers. Given this fact, the points of presence are divided, according to their importance, in three categories: (1) Class A sites - Command sites; (2)

Class B sites - Depots and Major Bases; and (3) Class C sites - other sites. This classification is used to set the type and speed of network connection. The costs of implementation were divided into three major categories: (1) hardware, software and Internet access costs, (2) maintenance costs, and (3) training and support costs. The final costs are a one-time setup cost of $400,730 and a monthly cost of $39,880. The payback period, after which the VPN solution is less expensive than the X.25 WAN, equals about 4 months.

Finally, the chapter discusses concepts of network security and emphasizes that, prior to the implementation of a network using the latest technologies, it is necessary to establish a complete security policy. The comparison of the X.25 solution with the VPN solution also reveals that, at a higher level of Information Warfare, both have the same vulnerabilities, whereas, at a lower level of Information Warfare, the VPN solution is exposed more threats, such as probing, exploitation of virii, and attacks from outside.

V. Conclusions and Recommendations

Chapter Overview

The objective of this chapter is to draw conclusions about the use of X.25 dedicated links and a Virtual Private Network over the Brazilian Internet Infrastructure to support the requirements of the Brazilian Air Force Materiel Command. This is accomplished by discussing the rationale of the assumptions used in this research, in order to understand their relation to the conclusions here presented, and to consider the implications of the research for the Brazilian Air Force. Finally, possible topics for future research are explored.

Conclusions and Recommendations

Regarding the implementation of the X.25 Brazilian Air Force WAN, Table 5.1 shows that one-time setup costs equal \$104,050, and monthly costs equal of \$121,476; in other words, the respective costs are the same order of magnitude. Table 5.1 also shows that 91.4% of one-time setup costs are attributed to hardware costs. This statistic reveals that hardware is a major cost factor. In similar way, 95.5% of

monthly costs are attributed to network access costs, also meaning that network access is a major cost factor.

Table 5.1 - Summary of Costs of X.25 and Associated Percentages

Category	One-time setup		Monthly	
Hardware	$95,050	91.4%	-	0%
Software	-	0%	-	0%
Network Access	-	0%	$115,976	95.5%
Maintenance	-	0%	$490	0.4%
Training	$9,000	8.6%	-	0%
Support		0%	$5,000	4.1%
TOTAL	**$104,050**	**100%**	**$121,466**	**100%**

Table 5.2 - Summary of Costs of a VPN and Associated Percentages

Category	one-time setup		Monthly	
Hardware	$122,050	30.5%	-	0%
Software	$108,000	27.0%	-	0%
Network Access	$10,680	2.7%	$29,780	74.7%
Maintenance	-	0%	$600	1.5%
Training	$60,000	15.0%	-	0%
Support	$100,000	25.0%	$9,500	23.8%
TOTAL	**$400,730**	**100%**	**$39,880**	**100%**

Regarding the implementation of a VPN-based solution, Table 5.2 shows that one-time setup cost equals $400,730, and monthly costs equals $39,980. Hence, these respective costs differ considerably in order of magnitude (one-time setup costs are approximately ten times greater than monthly costs). Table 5.2 also shows that one-time setup costs are evenly spread along four categories, which are hardware costs, software costs, training costs, and support costs. Moreover, 74.7% of monthly costs are attributed to network

access costs, while 23.8% are attributed to support costs. For this reason, network access can be considered a major cost factor.

Table 5.3 summarizes the previous conclusions:

Table 5.3 - Major Cost Factors

X.25 Model		VPN Model	
One-time setup	**Monthly**	**One-time setup**	**Monthly**
Hardware	Network Access	evenly spread among four factors	Network Access

Implications for the Brazilian Air Force

The cost conclusions in Tables 5.1, 5.2, and 5.3 have important implications for Brazilian Air Force's weapons systems. First of all, at the threshold of the twenty-first century, it is clear that information systems are playing an increasingly important role in providing improved logistics support both in the commercial and military sector. Therefore, the Air Force must use modern information systems in order to provide a high level of weapons systems availability and protect nation's welfare while staying within budget limits. Nowadays, to meet these challenges, the Brazilian Air Force is developing an information system called SILOMS (which stands for Logistics, Materiel, and Service Information Systems) which is expected to link the management of materiel, personnel, and logistic support

across all the major commands. Therefore, BAF could benefit from the implementation of a VPN, which provides a fast, reliable, and secure medium of data transmission that supports SILOMS's requirements.

The second conclusion is that the explosive (yet ordered) growth of the Internet implies that, in the near future, all information systems (including military systems) will be at least partially based on the Internet. Thus, any data transmission medium that ignores this fact will likely lead to several obstacles in maintaining that medium, finding spare parts for hardware, supporting software and finding new software, upgrading to meet new requirements, training personnel, and solving incompatibility problems with other media. Consequently, these obstacles will undoubtedly increase the overall cost of operating and supporting the medium. Therefore, the Brazilian Air Force can benefit from this research, which is a well-balanced perspective on the implementation of an X.25-based solution and a VPN-based solution.

The third is that it is necessary to find effective ways to guarantee the security of information systems. As the Internet grows, the number of Internet users able to "attack" an Internet-based military information system will increase. At the same time, however, the technology to

repel and counterattack these intruders improves. This is the environment in which the development of the VPN technology and the IPsec protocol fit. The Brazilian Air Force, when considering information as a very valuable asset, must recognize these facts. Therefore, this research helps educate decision makers by showing several methods of attack and their respective countermeasures for both X.25-based solution and VPN solution.

The final conclusion is that the cost breakdown structure adopted in this research suggests that the implementation of a VPN-based solution can lead to potential savings in the medium and long run. Figure 4.6 exhibits a payback period of approximately four months, meaning that for periods greater than four months, a VPN-based solution costs less than an X.25-based solution. Table 5.4 presents the savings for a five-year horizon and for a one-year horizon (a monthly inflation rate of 1% is used to calculate the net present value). According to Table 5.4, the Brazilian Air Force could save more than $ 600,000 within one year and more than $ 3 million within five years.

Table 5.4 - Potential Savings Along Planning Horizons

Category	X.25	VPN	Potential Savings
One-time setup costs	$104,050	$400,730	-
Monthly costs	$121,466	$39,880	-
Costs at the end of a one-year horizon (NPV)	$1,471,159	$849,582	**$621,577**
Costs at the end of a five-year horizon (NPV)	$5,564,559	$2,193,537	**$3,371,022**

Suggestions for Further Research

The results of Chapter IV, and the previous conclusions and implications suggests the following topics for future research:

1. A more detailed study could be done that considers the impact of recent privatization in the Brazilian telecommunication sector. In the recent past, the cost of owning a phone line was significantly reduced. More drastic reductions are expected in the next few years. At the same time, the speed and reliability of telecommunications services have increased. Together, these facts can cause a significant reduction of the costs of both X.25-based and VPN-based solutions.

2. Other Brazilian Air Force Major Commands could benefit from the implementation of a BAF-wide integrated VPN. The savings would be substantial, since not only DIRMA

(BAF's Materiel Command) would benefit, but other Major Commands as well, such as DIRSA (BAF's Health Services Command), DIRINT (BAF's Administrative Command), and DIRENG (BAF's Airport Engineering Command).

3. Future research could examine other networking alternatives such as Frame Relay and ATM, wireless communications, and Internet connections through other types of links (T1, T3, DDS). In addition, alternatives of VPN techniques such as SSL (Secure Socket Layer), Layer-2 Tunneling Protocol, PPTP (Point-to-Point Tunneling Protocol), and Socksv5 could be evaluated.

4. The measurement of the effective quality of service provided by Brazilian ISP's and the reliability of Internet carriers would be an interesting study. In addition, assessments of the likelihood of putting QoS terms in contracts of Internet Service Providers would be an interesting factor to consider in terms of cost of ISP services.

5. Research could be done to better estimate costs due to "hacker" attacks. This estimate would help to determine what type of attacks are more harmful, and which require more use of countermeasures. This research could be performed in parallel with the test of prototypes.

6. Prototype networks could be built to assess parameters such as availability, reliability, speed of connection, and frequency and nature of attacks. These prototypes would also help refine the cost estimates and structure.

7. The BAF network requirements (in terms of traffic) could be studied using the data available on the BAF's logistics support requisitions. Future studies could research the bandwidth necessary for the traffic of application data, along with other Internet services such as mailing, Web-hosting, and administrative tools.

8. This research could be expanded to address Global Information Warfare. In this case, special purpose systems specifically designed for Information Warfare are created, leading to the establishment of a whole new set of very high-level security requirements and countermeasures. However, enormous amount of resources (money, personnel, training, and facilities) would be necessary.

Closing Remarks

This research addressed the implementation of an X.25 WAN and the implementation of a Virtual Private Network over the Internet, as media of data transmission among the units belonging to DIRMA (Brazilian Air Force Materiel Command).

The objective was to determine which of the solutions presented was more capable of satisfying the requirements and needs of the Brazilian Air Force Materiel Command. For both solutions, the research provided an insight on the way costs are allocated, and how the media are affected by threats and "hacker" attacks. The research revealed that the most viable solution was the implementation of VPN over the Internet. Such solution, if implemented, would create significant savings in the medium and long run. Due to the dynamic nature of the cost data gathered, this research should be considered as a point estimate. Therefore, these cost results may not prove valid in the near future, although the cost breakdown structure adopted and the considerations on security will likely be valid for a longer time.

(Page intentionally left in blank)

Appendix A. List of Acronyms and Abbreviations

ARPANET	Advanced Research Projects Agency Network
ATM	Asynchronous Transfer Mode
BAF	Brazilian Air Force
BPS	bits per second
C/S	Client/Server
C3	Command, Control and Communications
C3I	Command, Control, Communications, and Intelligence
CERT	Computer Emergency Response Team
DEPV	Brazilian Air Force Air Traffic Directorate (Departamento de Proteção ao Vôo)
DES	Data Encryption Standard (USA)
DH	Diffie-Hellman (public encryption scheme)
DIRINFE	Brazilian Air Force Computer Science and Statistics Directorate (Diretoria de Informática e Estatística)
DIRMA	Brazilian Air Force Materiel Command (Diretoria de Material)
DISA	Defense Information Systems Agency (USA)
DoD	Department of Defense (United States of America)
EFF	Electronic Frontier Foundation
IDEA	International Data Encryption Algorithm
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPX	Internetwork Packet Exchange (Novell Proprietary)
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IT	Information Technology
IW	Information Warfare
EMBRATEL	Brazilian Telecommunications Company (Empresa Brasileira de Telecomunicações)
LAN	Local-Area Network
MA	Maintenance Actions
MTBF	Mean-Time Between Failures

NETBEUI	NETBIOS Extended User Interface
OSI	Open Systems Interconnection
PPTP	Point-to-point Tunneling Protocol
QoS	Quality of Service
RADIUS	Remote Access Dialup User Service
RCDMA	Brazilian Air Force Data Communications Network (Rede de Comunicação de Dados do Ministério da Aeronáutica)
RENPAC	Brazilian Internet Backbone (Rede Nacional de Pacotes)
SILOMS	Brazilian Air Force Logistics, Materiel, and Services Information System (Sistema Integrado de Logística Material e Serviços)
SISMA	Brazilian Air Force Materiel System (Sistema de Material)
TBF	Time Between Failures
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide-Area Network
WWW	World Wide Web
X.25	The CCITT protocol standard that specifies the interface between host systems and a packet-switching network

Appendix B: Brazilian Air Force Material System Units

BRAZILIAN AIR FORCE UNITS						Geodesic	TRANSDATA
Unit	Description	City	State	Class	ISP	Distance	Monthly $
AFA	Air Force Academy	Pirassununga	SP	C	lancernet.com.br	5	$1,036.62
BAAF	Afonsos Air Force Base	Rio de Janeiro	RJ	C	homeshopping.com.br	1	$459.57
BAMN	Manaus Air Force Base	Manaus	AM	C	nutecnet.com.br	8	$1,394.26
BAAN	Anápolis Air Force Base	Anápolis	GO	C	genetic.brnet.com.br	3	$649.62
BABE	Belém Air Force Base	Belém	PA	C	homeshopping.com.br	1	$459.57
BABR	Brasília Air Force Base	Brasília	DF	C	homeshopping.com.br	1	$459.57
BABV	Boa Vista Air Force Base	Boa Vista	RR	C	technet.com.br	7	$1,285.40
BACG	Campo Grande Air Force Base	Campo Grande	MS	C	cgr.nutecnet.com.br	7	$1,285.40
BACO	Canoas Air Force Base	Canoas	RS	C	conetsul.com.br	1	$459.57
BAFL	Florianópolis Air Force Base	Florianópolis	SC	C	unetsul.com.br	5	$1,036.62
BAFZ	Fortaleza Air Force Base	Fortaleza	CE	C	homeshopping.com.br	8	$1,394.26
BAGL	Galeão Air Force Base	Rio de Janeiro	RJ	C	homeshopping.com.br	1	$459.57
BAPV	Porto Velho Air Force Base	Porto Velho	RO	C	enter-net.com.br	8	$1,394.26
BARF	Recife Air Force Base	Recife	PE	C	homeshopping.com.br	1	$459.57
BASC	Santa Cruz Air Force Base	Rio de Janeiro	RJ	C	homeshopping.com.br	1	$459.57
BASM	Santa Maria Air Force Base	Santa Maria	RS	C	smnet.com.br	4	$882.86
BASP	São Paulo Air Force Base	Guarulhos	SP	C	homeshopping.com.br	1	$459.57
BAST	Santos Air Force Base	Santos	SP	C	unimes.com.br	4	$882.86
BASV	Salvador Air Force Base	Salvador	BA	C	stn.com.br	6	$1,152.39
CABE	European Aeronautical Commission	London	UK	B	ibm.net.uk	8	$1,394.26
CABSP	São Paulo Aeronautical Commission	São Paulo	SP	B	embratel.net.br	1	$459.57
CABW	Washington Aeronautical Commission	Washington	USA	B	prodigy.net	8	$1,394.26
CATRE	Trainning Command	Natal	RN	C	homeshopping.com.br	5	$1,036.62
MINAER	Air HQ + Materiel HQ	Brasília	DF	A	embratel.net.br	1	$459.57
CTA	Aerospacial Technical Center	São José dos Campos	SP	B	embratel.net.br	4	$882.86
DARJ	Aeronautical Deposit	Rio de Janeiro	RJ	C	homeshopping.com.br	1	$459.57
DIRINFE	Computer Systems Command	Rio de Janeiro	RJ	A	embratel.net.br	1	$459.57
DIRMA	Air Force Materiel Command	Rio de Janeiro	RJ	A	embratel.net.br	1	$459.57
DIRMAB	Weapons Materiel Command	Rio de Janeiro	RJ	B	embratel.net.br	1	$459.57
PAMAAF	Afonsos Aeronautical Depot	Rio de Janeiro	RJ	B	embratel.net.br	1	$459.57
PAMABE	Belém Aeronautical Depot	Belém	PA	C	homeshopping.com.br	8	$1,394.26
PAMAGL	Galeão Aeronautical Depot	Rio de Janeiro	RJ	B	embratel.net.br	1	$459.57
PAMALS	Lagoa Santa Aeronautical Depot	Lagoa Santa	MG	B	embratel.net.br	1	$459.57
PAMARF	Recife Aeronautical Depot	Recife	PE	B	embratel.net.br	8	$1,394.26
PAMASP	São Paulo Aeronautical Depot	São Paulo	SP	B	embratel.net.br	1	$459.57
PAMBE	Weapons Depot	Rio de Janeiro	RJ	B	embratel.net.br	1	$459.57
							$28,622.90

Appendix C: Cost Breakdown Structure

Hardware	**Development**
Servers	Graphic design and user interfaces
Routers	Site analysis and design consulting
Workstations	Basic content coding
Hubs	Special applications
Other Hardware	Database Integration
Software	Other development costs
Server Software	**Training**
Client Software	Partner Training
Database Software	Employee Training
Firewall Software	Design of Training Courses
Version Control Tools	Ongoing Training
Content Development Tools	Other Training Costs
Commerce Software	**Maintenance**
E-mail software	Server Backup Labor
Telecommunications Software	Server Backup tapes/equipment
Other Software	Hardware Servicing
Internet Connection	Software Upgrades
Telecom Line - Installation	Other Maintenance
Telecom Line - Monthly Circuit Usage	**Support**
Internet Access - Installation	Help Desk Design and Consulting
Internet Access - Monthly Charges	Help Desk Implementation
Other Costs	Bug Tracking System
Server/Site Hosting	Bug Tracking Implementation
Server co-location/site hosting	Beta Test Support
Site/Server Maintenance	System Administrator Salary
Security	Other Support Costs
Firewall Machine	**Management**
Security Audit	Project management
RSA Certificates	Outside Consulting
Routers	Webmaster
Site Security Officer Salary	Other management costs
Other security and staffing costs	**Depreciation**

Source: [24]

Appendix D: Encryption Algorithms

Symmetric Algorithms and One-Way Hash Functions

Algorithm	Type	Clocks per byte Processed (Pentium)	Block size (bytes)	Key size (bytes)	Patents
RC4	Stream	7	N/A	Variable	No
Blowfish	Block	18	8	4-56	No
CAST	Block	20	8	16	Yes, but free
RC5-32/16	Block	23	8	Variable	Pending
DES	Block	45	8	7	No
IDEA	Block	50	8	16	Yes
SAFER	Block	52	8	16	No
3-DES	Block	108	8	14	No
MD5	Hash	5	64	N/A	No
SHA-1	Hash	13	64	N/A	No
RIPE-MD-160	Has	16	64	N/A	No

Committed Resources to Crack an encryption algorithm

Type of Attacker	Budget	Tool	40 bits: Time and Cost per key recovered	56 bits: Time and Cost per key recovered	Key length for protection in late 1996
Pedestrian hacker	Tiny $400	Scavenged Computer FPGA	1 week (no cost) 5 hours ($0.08)	Unfeasible (no cost) 38 years ($5000)	45 50
Small Business	$10,000	FPGA	12 minutes ($0.08)	556 days ($5,000)	55
Corporate Department	$ 300K	FPGA ASIC	24 seconds ($0.08) 0.18 seconds ($0.001)	19 days ($5,000) 3 hours ($38)	60 60
Big Company	$ 10M	FPGA ASIC	0.7 seconds ($0.08) 0.005 seconds ($0.001)	13 hours ($ 5,000) 6 minutes ($38)	70 70
Intelligence agency	$ 300M	ASIC	0.0002 seconds ($0.001)	12 seconds ($38)	75

FPGA - Field-Programmable Gate Array;
ASIC - Application-Specific Integrated Circuits
Source: [49]

Appendix E. Benchmark of Commercial Firewalls and VPN Solutions

	Aventail VPN 2.5	CheckPoint FireWall-1 3.0a	Raptor Eagle NT 4.0
VPN Features			
Supports LAN-to-LAN	Yes	Yes	Yes
Supports Client-to-LAN	Yes	Yes	Yes
Supports Client-to-Client			
Supports PPTP			
Supports compression			
IP payloads	Yes	Yes	Yes
IPX/NetBEUI payloads			
Supports IPv6 carrier	Yes		
Supports IPSec (RFC 1825)	Yes	Yes	Yes
Supports SKIP key management		Yes	
Other key management	Yes	Yes	Yes
Supports multiple tunnels from single server	Yes	Yes	Yes
Supports multiple tunnels from single client	Yes	Yes	Yes
Encryption Features			
RSA	Yes	Yes	
DES	Yes	Yes	Yes
Triple-DES	Yes	Yes	Yes
IDEA			
Blowfish			
RC2			Yes
RC4	Yes	Yes	
Diffie-Hellman	Yes	Yes	
MD4	Yes		
MD5	Yes	Yes	Yes
SHA-1	Yes	Yes	Yes
Full strength available for unlimited export			
Supports automatic key exchange during session	Yes	Yes	
Support Encryption on a service-by-service basis	Yes	Yes	

	Aventail VPN 2.5	CheckPoint FireWall-1 3.0a	Raptor Eagle NT 4.0
Management and administration			
Manage access by level group	Yes	Yes	
SNMP-manageable		Yes	Yes
Remote manage via HTTP			
Remote manage via Java			
Remote manage via other		Yes	Yes
Directory support for LDAP			
Directory support for NDS	Binder only	Directory File Import	Directory File Import
Other directory support	NT Domain	Yes	
Includes client software			
Client/Server Support			
Windows 3.x	Client		Client
Windows 95	Client	Client	Client
Windows NT	C/S	C/S	C/S
Solaris	C/S	Server	Server
BSD	C/S		
Other Unix	C/S	Server	Server
Authentication Features			
CHAP/PAP	Yes		
RSA			
RADIUS	Yes	Yes	Yes
S/Key		Yes	Yes
SecurID	Yes	Yes	Yes
Other token authentication		Yes	Yes
SSL	Yes		
Support Filters	Yes	Yes	Yes
Authentication by IP address		Yes	Yes

Sources: [53, 67]

Appendix F. RENPAC 3025 prices table (EMBRATEL)

Date: October 1st, 1997

1. DEDICATED ACCESS							
1.2 PORT (TYPE 2) AND PORT / ACCESS (TYPE 1)							
RENPAC - 3025 (X.25) - MAXIMUM MONTHLY RATE - R$ - TAX: ICMS = 25%, PASEP = 0,65% AND COFINS = 2,00%							
SPEED IN KBPS	PERMANENT (**)	TEMPORARY - (***) - CONTRACT 1 – 30 DAYS (3 / 4)					
	CONTRACT GREATER THAN 30 DAYS	1 - 5 DAYS	6 DAYS	7 DAYS	8 DAYS	9 DAYS	10 - 30 DAYS
2.4 (1)	313.69	156.84	188.21	219.58	250.95	282.32	313.69
4.8 (1)	354.84	177.42	212.90	248.39	283.87	319.36	354.84
9.6 (1)	382.48	191.24	229.49	267.74	305.99	344.23	382.48
19.2 (1)	465.41	232.70	279.25	325.79	372.33	418.87	465.41
64 (1)	1,167.62	583.81	700.57	817.34	934.10	1,057.86	1,167.62
64 (2)	761.20	380.60	456.72	532.84	608.96	685.08	761.20
128 (2)	1,747.54	873.77	1,048.52	1,223.28	1,398.03	1,572.79	1,747.54
256 (2)	2,454.55	1,227.27	1,472.73	1,718.18	1,963.64	2,209.09	2,454.55
512 (2)	3,447.14	1,723.57	2,068.28	2,413.00	2,757.71	3,102.43	3,447.14
2 M (2)	11,586.49	5,793.24	6,951.89	8,110.54	9,269.19	10,427.84	11.586.49

1.4 REMOTE ACCESS UP TO 64 KBIT/s (TYPE 1) (OUT OF THE BASIC TARIFFATION AREA)			
PRICES SHOULD BE APPLICATED IN ADDITION TO THE LOCAL CARRIER TARIFFS			
DEGREE		GEODESIC DISTANCE (IN KM)	MONTHLY PRICE - R$ - (5) TAXES INCLUDED ICMS = 25%, PASEP = 0.65% e COFINS = 2.0%
OLD	NEW		
02	01	UP TO 50	0,00 (6)
03	02	FROM 50 TO 100	214.88
04	03	FROM 100 TO 200	275.07
05	04	FROM 200 TO 300	315.53
06	05	FROM 300 TO 500	376.06
07	06	FROM 500 TO 700	390.75
08	07	FROM 700 TO 1000	400.53
09	08	FROM 1000 TO 1500	420.27
10	08	GREATER THAN 1500	420.27

NOTES:
(5) - Values are valid for remote access for national and international RENPAC calls (all prices already contain respective taxes).
(6) - Inside the Basic Tariff Area (ATB RENPAC).

2. PORTS 3025	
TRANSMISSION SPEED IN BPS	MONTHLY PRICE - R$ (7) Applicable taxes included ICMS = 25%, PASEP = 0.65% e COFINS = 2.0% (No Local Line and Modem)
2400	193.62
4800	234.77
9600	262.41
19200	331.31

(7) Values valid for ports used in domestic and international calls. Franchise of R$ 106.50.

3. DOMESTIC TRAFFIC UTILIZATION

3.1. BY THE VOLUME RECEIVED AND TRANSMITTED

CLASS	MAXIMUM TARIFF - R$ - (8) WITH APPLICABLE TAXES (ICMS = 25%, PASEP = 0.65% e COFINS = 2.0%)			
	NORMAL		REDUCED	
	MINIMAL UTILIZATION (9)	ADITTIONAL SEGMENT	MINIMAL UTILIZATION (9)	ADDITIONAL SEGMENT
	4 SEGMENTS BY CALL	BY SEGMENTS OF 64 OCTETS	4 SEGMENTS BY CALL	BY SEGMENTS OF 64 OCTETS
LOCAL	0.00154	0.00038	0.00077	0.00019
01	0.00160	0.00040	0.00077	0.00019
02	0.00221	0.00055	0.00110	0.00027
03	0.00403	0.00100	0.00199	0.00049
04	0.00409	0.00102	0.00204	0.00051
05	0.00552	0.00138	0.00276	0.00069
06	0.00630	0.00157	0.00315	0.00078
07	0.00657	0.00164	0.00326	0.00081
08	0.00691	0.00172	0.00342	0.00085

(9) Incomplete or complete call

3.1.1. TARIFF DISCOUNTS BY UTILIZATION VOLUME

3.1.2. DISCOUNT BY VOLUME RECEIVED AND SENT

MONTHLY TRAFFIC IN MILLION OF SEGMENTS	% DISCOUNT
UP TO 5	0
FROM 5 TO 10	5
FROM 10 TO 15	10
FROM 15 TO 20	15
FROM 20 TO 60	20
FROM 60 TO 100	30
FROM 100 TO 145	40
FROM 145 TO 200	45
HIGHER THAN 200	50

OBS.: INTERNATIONAL TRAFFIC IS NOT ACCOUNTED FOR DISCOUNT PURPOSES

4. DISCOUNTS FOR CONTRACTS WITH INDETERMINED PERIOD

CONTRACT VALUE (MINIMUM MONTHLY CHARGE) - R$	DISCOUNT IN THE PERIOD (%)	
	3 ANOS	5 ANOS
20.000,00	3	5
50.000,00	6	10
100.000,00	9	15
200.000,00	12	20
400.000,00	15	25

1. INTERNATIONAL TRAFFIC RATES

1.1 VOLUME

FOR EACH SEGMENT OF 64 OCTETS	FEE UNITARY - R$	0,01316

Sources: [56, 58]

BIBLIOGRAPHY

1. General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Report GAO/AIMD-96-84. Washington: GAO, May 1996.

2. Hundley, R.O. and R.H. Anderson Security in Cyberspace - an emerging challenge for society. RAND Report P-7893. RAND Corporation, December 1994.

3. Brazilian Air Force. "Description of the Brazilian Air Force Information System." WWWeb, http://www.maer.mil.br. August 1998.

4. Heterick, Robert C. Jr. "Creative Destruction" Educom Review, 32(1): 18 (May/June 1997).

5. Hurwicz, Mike. "A Virtual Private Affair," Byte Magazine, 22(7): 79-87 (July 1997).

6. Stern, Morgan. "Extend Your Net with VPNs," Byte Magazine, 22(11): 114-119 (November 1997).

7. Smith, Veronica. "Plan Ahead," Communications Week, 610: 49-54 (May 1996).

8. Blaze, M. et al. Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security. Counterpane Systems, Minneapolis MN (January 1996).

9. Udell, Jon. "Your business needs the web," Byte Magazine 21(8): 68-80 (August 1996).

10. Stallings, William. Data and Computer Communications (Fifth edition). Upper Saddle River: Prentice Hall Editor, 1997.

11. Loshin, Pete. "Extranets Reach the Spotlight" Byte 23(1): 71 (January 1998).

12. Donlon, Matt. "Extranet for Security Professionals." WWWeb, http://isp.hpc.org/. (June 1998)

13. Kujubu, Laura. "MCI to reveal consolidated VPN services," Infoworld, 19(49): 08 (December 1997).

14. Lawson, Stephen. "Waiting for VPN's payoff," Infoworld, 20(4): 103 (January 1998).

15. Hoffman, Thomas. "Transaction Action" Computerworld, 31(46): 14 (November 1997).

16. Wallace, Bob. "Net helps wither winery phone costs," Computerworld, 32(19): 51-52 (May 1998).

17. Wallace, Bob. "Virtual Private Network saves firms big money," Computerworld 31(31): 49-50 (August 97).

18. Riggs, Brian. "Can you trust the Internet?" LAN Times, WWWeb, http://www.lantimes.com/97/97sep/709b001b.html. September 1997.

19. Cray, Andrew. "Secure VPN: Lock the Data, Unlock the Savings," Data Communications 26(7): 49-56 (May 1997).

20. Davis, Beth et al. "VPNs: Virtually Unstoppable," Information Week 658: 18 (November 1997).

21. Tate, Priscilla. "Internet Security: can best practices overcome worst perils?" Computerworld Technology Forum, Special Brochure, (May 1998).

22. Schneier, Bruce. Applied Cryptography (2nd edition). New York: John Wiley & Sons, Inc., 1996.

23. Schwartau, Winn. Information Warfare (2nd edition). New York: Thunder's Mouth Press, 1996.

24. Bayles, Deborah. Extranets - Building the Business to Business Web. Upper Saddle River NJ: Prentice Hall, 1998.

25. Washburn, K. and J.T. Evans TCP/IP Running a Successful Network. Padstow, New South Wales: Addison-Wesley, 1993.

26. Hughes Jr., Larry J. Internet Security Techniques Indianapolis: New Rider Publishers, 1995.

27. Pfaffenberger, Brian. Building a Strategic Extranet Foster City CA: IDG Books, 1998.

28. Hare, C. and Karanjit Siyan. Internet Firewalls and Network Security (2nd edition). Indianapolis: New Riders Publishing, 1996.

29. Anonymous. Maximum Security, Indianapolis: Sams Net, 1997.

30. Klander, Lars. Hacker Proof. Las Vegas: Jamsa Press, 1997.

31. Garfinkel, S. and G. Spafford. Practical Unix & Internet Security (2nd edition). Sebastopol CA: O'Reilly & Associates, Inc., 1996.

32. Computer Emergency Response Team. Ongoing Network Monitoring Attacks. CERT Advisory Report CA-94:01. February 1994. (ftp://info.cert.org/pub/cert_advisories)

33. Guha, Biswaroop and Biswanath Mukherjee. "Network Security via Reverse Engineering of TCP Code: Vulnerability Analysis and Proposed Solutions," IEEE Network 11(4): 40 (July 1997).

34. Morris, Robert T. A Weakness in the 4.2BSD Unix TCP/IP Software. AT&T Bell Laboratories: Murray Hill NJ, 1985.

35. Newmann, D. and others. "Firewalls: Don't Get Burned," Data Communications 26(4): 37-53, (March 1997).

36. Lipschutz, R.P. "Safety from the Net" PC Magazine, 16(20): 243-263 (November 1997).

37. Lipschutz, R.P. "Net Protection," PC Magazine, 17(7): 229-230 (April 1998).

38. Ahuja, Vijah. Network & Internet Security. Chestnut Hill MA: AP Professional Editors, 1996.

39. Computer Emergency Response Team. IP Spoofing Attacks and Hijacked Terminal Connections. CERT Advisory Report CA-95:01. January 1995. (ftp://info.cert.org/pub/cert_advisories)

40. DiDio, Laura. "Federal agencies fail security test," Computerworld, 32(21): 16 (May 1998).

41. US Department of Defense. Trusted Computer Systems Evaluation Criteria. DoD Directive 5200.28-STD. Washington: U.S. Government Printing Office, 1985.

42. Cheswick, William R. and Steven M. Bellovin. Firewalls and Internet Security. Reading MA: Addison-Wesley Publishing Co, 1994.

43. Sutton, Steve. Microsoft Product Security - An Overview. Microsoft Corporation, September 1997.

44. Stinson, Douglas R. Cryptography - Theory and Practice. Boca Raton FL: CRC Press, 1995.

45. CheckPoint Software Technologies Task Group. Virtual Private Network Security Components. CheckPoint Software Technologies Ltd., 1998

46. Rosen, Michele. "Internet Security Standards," PC Magazine, 17(2): 241, (January 1998).

47. Cray, Andrew "Encryption," Data Communications, 25(17): 44-52 (December 1996).

48. Kerstetter, J. "Quick Crack Dooms DES," PC Week, 15(31): 26 (August 1998).

49. Schneier, Bruce. "The Crypto Bomb is Ticking," Byte Magazine, 23(105): 97-102 (May 1998).

50. CheckPoint Software Technologies Task Group. Virtual Private Network Security Components. CheckPoint Software Technologies, March 1998.

51. Rede Nacional de Pesquisa. "RNP Descrição da Rede." WWWeb, http://www.rnp.br/1.3.desc.html. (March 1998).

52. Rede Nacional de Pesquisa. "RNP Histórico." WWWeb, http://www.rnp.br/1.3.hist.html. (March 1998).

53. Greenfield, David. "Global Intranet Services – Patchy but Promising," Data Communications 26(4): 77-82, (March 1997).

54. Campbell, Ian. "The Intranet: Slashing the Cost of Business." International Data Corporation, Netscape Corporation Web Page. WWWeb, (http://home.netscape.com/comprod/announce/idc/summary.html), (June 1998).

55. Anthes, Gary H. "Talking over the 'net saves company cash," Computerworld, 29(50): 63-69 (December 1995).

56. Embratel Task Group. Serviços RENPAC 3025/RENPAC 3028/RENPAC 3030. Brasilia: Embratel, April 1998.

57. CISCO Product Catalog Web-page. "Cisco 2505 and 2507 Router/Hubs." WWWeb, http://www.cisco.com/warp/public/558/19.html (August 1998).

58. 3Com Product Catalog Web-page "SuperStack II NETBuilder Remote Office Router Family." WWWeb, http://www.3com.com/products/dsheets/400159.html (August 1998).

59. Digi International Product Catalog. Digi International MN, Spring 1998.

60. Babcock, Charles. "The Art of Building VPN Firewalls," Interactive Week 5(29): 18 (August 1998).

61. Broderick, J. et al. "Remote access: VPN vs. dial-up - VPN growing pains," WWWeb, http://www.infoworld.com/cgi-bin/displayTC.pl?/97btc.sid1.htm. (December 1997).

62. Bruno, Lee "Internet Security: How much is enough?," Data Communications, 25(5): 60-72 (April 1996).

63. Atkinson, R. Request for Comment 1825 - Security Architecture for the Internet Protocol. IETF Networking Group, Aug 1995.

64. Cheswick, Bill. The Design of a Secure Internet Gateway. Murray Hill NJ: AT&T Bell Laboratories.

65. Bird, Tina. VPN Implementation Case Study. Secure Network Systems Inc, January 1998.

66. Larsen, Amy K. "All Eyes on IP Traffic," Data Communications, 26(4): 59-102 (March 1997).

67. CheckPoint Software Task Force. "Product Description - Firewall-1 Solution." WWWeb, http://www.checkpoint.com/products/firewall-1/descriptions/encryption.html. (July 1998).

68. Embratel. "Transdata - Descrição de Serviços." WWWeb, http://www.embratel.com.br/servicos/transdata.html, (March 1998).

69. Farmer, Dan and Wietsie Venema. Improving the Security of your site by breaking into it. Sun Microsystems Inc., Palo Alto CA, 1994

70. Sterling, Bruce "Short History of the Internet," The Magazine of Fantasy and Science Fiction, 84#2(501): 99-107 (February 1993).

71. Drew, Dale. Protection of TCP/IP Based Network Elements. MCI Telecommunications Inc., 1995.

72. Rowland, Craig H. Covert Channels in the TCP/IP Protocol Suite. Psionic Corporation, 1996.

73. Computer Emergency Response Team. IP Denial-of-Service Attacks. CERT Advisory Report CA-97:28. May 1996. (ftp://info.cert.org/pub/cert_advisories)

74. Computer Emergency Response Team. TCP SYN Flooding and IP Spoofing Attacks. CERT Advisory Report CA-96:21. September 1996. (ftp://info.cert.org/pub/cert_advisories)

75. Computer Emergency Response Team. Sendmail Vulnerabilities. CERT Advisory Report CA-96:20 September 1996. (ftp://info.cert.org/pub/cert_advisories)

76. Psionic Corporation Task Group. "Common System Intrusion Methods." WWWeb, http://www.psionic.com/papers/attacks.html,(December 1997).

77. Barksdale, Jim. From ARPANET to Intranet: the U.S. Government and Internet Technologies. Netscape Corporation, Mountain View CA, September 1996.

78. Hamzeh et al. "Point-to-Point Tunneling Protocol - PPTP." Internet Engineering Task Group, July 1997.

79. Lebano, Tito N. A TCP/IP Gateway Interconnecting a X.25 Packet Radio Network to the Defense Data Network. MS thesis, AFIT/GCS/ENG/88D-25. School of Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, 1988 (AD-A202733).

80. Conres, Douglas E. Internetworking with TCP/IP, Volume I (3rd edition) Englewood Cliffs NJ: Prentice Hall Editors, 1995.

81. Chan, Mun C. et al. An Architecture for Externally Controllable Virtual Networks and its Evaluation on NYNet. Rome Laboratory - USAF Materiel Command Technical Report RL-TR-97-76. New York: Government Printing Office, August 1997.

82. Henriksen, Gene. Windows NT and Unix Integration, Indianapolis: Macmillan Tehnical Publishing, 1998.

83. Microsoft Corporation Task Group. Microsoft Corporation Internet Information Server Resource Kit. Redmond WA: Microsoft Press, 1998.

84. Brazilian Air Force - Electronic Warfare Center. WWWeb, http://www.maer.mil.br/comgar/cgegar/index.html, August 1998.

85. Microsoft Corporation Task Group. Networking Essentials (2nd edition) Redmond WA: Microsoft Press, 1998.

86. Microsoft Corporation Task Group. Microsoft Internet Information Server 4.0 Training Kit. Redmond WA: Microsoft Press, 1997.

87. Electronic Frontier Foundation. Cracking DES. Sebastopol CA: O'Reilly & Associates, 1998.

Vita

1st Lieutenant Luiz Gustavo Silva was born on 29 September 1970 in Niterói, RJ, Brazil. He graduated from M. C. Centro Educacional de Niterói (CEN) High School in 1988 and entered undergraduate studies at the Technological Institute of Aeronautics (ITA) in São José dos Campos, SP, in 1989. In 1990, by a cooperation between the Brazilian Air Force and the Brazilian Army, he went to the Army's Engineering Institute (IME) in Rio de Janeiro, RJ, Brazil. He received his commission on 01 January 1990, and graduated with a Bachelor of Science degree in Chemical Engineering in December 1993. He was then assigned to Recife Aeronautical Materiel Depot (PAMARF), where he worked first as Maintenance Officer responsible for the shops of manufacture and maintenance, and later as Planning and Control Officer, where he developed a local maintenance system (SIMA) based on MS Visual Basic and Access database. In June 1996 he went to the Brazilian Air Force Institute of Logistics in order to make the Extension in Logistics course, in which he completed as the first place; and then, in March 1997 he entered the Graduate School of Logistics and Acquisition Management, Air Force Institute of Technology, and will move

on to the Brazilian Air Force Institute of Logistics (ILA) at São Paulo AFB, SP, Brazil, upon graduation in September 1998.

Forwarding Address: Av. Monteiro Lobato, 4455 - Cumbica
CEP 07184-000 Guarulhos - SP
Brazil

Vita

1st Lieutenant Alexandre Lima Guerra was born on 04 November 1970 in São Paulo, SP, Brazil. He graduated from M. C. Dr Américo Brasiliense High School in 1987 and entered undergraduate studies at the Technological Institute of Aeronautics (ITA) in São José dos Campos, SP, in 1988. He received his commission on 01 January 1990, and graduated with a Bachelor of Science degree in Aeronautical Engineering in December 1992. He was then assigned to São Paulo Aeronautical Materiel Depot (PAMASP), where he worked first as Maintenance Officer of the Aircraft Northrop F-5E, and later as Maintenance Officer of the aircraft EMB-120 Brasília. In June 1996, he went to the Brazilian Air Force Institute of Logistics in order to attend the course on Extension in Logistics, which he completed in December 1996. In March 1997, he entered the Graduate School of Logistics and Acquisition Management, Air Force Institute of Technology, and will move on to the Brazilian Air Force Institute of Logistics (ILA) at São Paulo AFB, SP, Brazil, upon graduation in September 1998.

Forwarding Address: Av. Monteiro Lobato, 4455 - Cumbica
CEP 07184-000 Guarulhos - SP
Brazil

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE
September 1998

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE
FEASIBILITY STUDY ON THE USE OF THE INTERNET FOR TRAFFIC OF UNCLASSIFIED DATA

5. FUNDING NUMBERS

6. AUTHOR(S)
Alexandre L. Guerra, Lieutenant, Brazilian Air Force
Luiz G. Silva, Lieutenant, Brazilian Air Force

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
2750 P Street
WPAFB, OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GLM/LAL/98S-7

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N / A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 Words*)

This research compares two possible networking methods for connecting all Brazilian Air Force Materiel Command units responsible for support and operation of Brazilian Air Force's weapons systems. The network includes the use of dedicated X.25 links, and the use of a Virtual Private Network using the Internet (TCP/IP) as the medium of transmission. The Brazilian Air Force Materiel Command, responsible to support operating units over a very large sparse territory, lacks an efficient media of computer communications, which makes it difficult to control the supply-chain channels of materiel present in each unit, depots, and warehouses. We studied the network infrastructure necessary to solve this problem, and proposed two different scenarios. One uses the current level of technology based on dedicated X.25 environment, and the other uses the incipient Virtual Private Networking technology and the Internet as the communication medium. The results suggest that the Brazilian Air Force could be able to use the Internet and VPN technology in a moderated secure environment (C2 Level), and could save more than $ 100,000 per month in comparison to the implementation of the same level of networking using the present X.25 model.

This study concludes that the BAF may benefit from the use of the VPN model in a secure and less costly environment, while maintaining the necessary flexibility and high performance to operate in the newly paradigm of distributed environments. Other implications for the Brazilian Air Force regarding Information Warfare issues and recommendations for further study are discussed.

14. SUBJECT TERMS
TCP/IP, Internet protocol, data security, Brazilian Air Force, network, Virtual Private Networks, attacks, threats, Information Warfare

15. NUMBER OF PAGES
160

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

AFIT Control Number AFIT/GLM/LAL/98S-7

AFIT RESEARCH ASSESSMENT

The purpose of this questionnaire is to determine the potential for current and future applications of AFIT thesis research. **Please return completed questionnaire** to: AIR FORCE INSTITUTE OF TECHNOLOGY/LAC, 2950 P STREET, WRIGHT-PATTERSON AFB OH 45433-7765. Your response is **important.** Thank you.

1. Did this research contribute to a current research project? a. Yes b. No

2. Do you believe this research topic is significant enough that it would have been researched (or contracted) by your organization or another agency if AFIT had not researched it?
a. Yes b. No

3. **Please estimate** what this research would have cost in terms of manpower and dollars if it had been accomplished under contract or if it had been done in-house.

Man Years____________ $____________

4. Whether or not you were able to establish an equivalent value for this research (in Question 3), what is your estimate of its significance?

a. Highly Significant b. Significant c. Slightly Significant d. Of No Significance

5. Comments (Please feel free to use a separate sheet for more detailed answers and include it with this form):

Name and Grade

Organization

Position or Title

Address